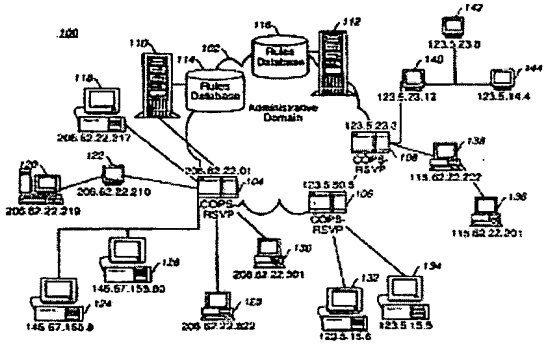
Customer resources policy control for IP traffic delivery

Publication number: CN1409823
Publication date: 2003-04-09
Inventor: RAWLINS D J (US); DONOVAN S R (US); GALLANT J K (US)
Applicant: MCI WORLDCOM INC (US)
Classification:
- International: ***H04L12/56;*** **H04L12/56;** (IPC1-7): G01R31/08
- European: H04L12/56D5; H04L12/56D5R
Application number: CN20008017065 20001012
Priority number(s): US19990416101 19991012

Also published as:
WO0127644 (A1)
US7106756 (B1)
MXPA02003722 (A)
EP1257835 (A0)
CA2387449 (A1)

Abstract not available for CN1409823
Abstract of corresponding document: **WO0127644**

A method, system, and computer program product for controlling customer resources for Internet protocol (IP) traffic delivery are disclosed. The network utilization of a group of endpoints on a network is tracked to generate group utilization level information corresponding to a current amount of network resource consumption by the group of endpoints. A request for network resources for a data flow for an endpoint in the group is received from a router associated with that endpoint. The request for network resources includes an identifier associated with the endpoint. A determination is made whether to accept the request based on the group utilization level information, the identifier, and a first predetermined profile associated with the group and including a first network utilization limit.



[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
G01R 31/08

[12] 发明专利申请公开说明书

[21] 申请号 00817065.7

[43] 公开日 2003 年 4 月 9 日

[11] 公开号 CN 1409823A

[22] 申请日 2000.10.12 [21] 申请号 00817065.7
[30] 优先权
[32] 1999.10.12 [33] US [31] 09/416,101
[86] 国际申请 PCT/US00/28232 2000.10.12
[87] 国际公布 WO01/27644 英 2001.4.19
[85] 进入国家阶段日期 2002.6.12
[71] 申请人 MCI 全球通讯公司
地址 美国密西西比州
[72] 发明人 D·J·劳林斯 S·R·多诺范
J·K·加兰特

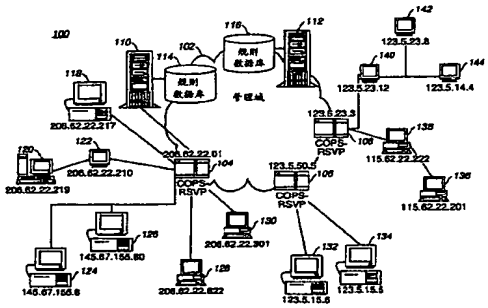
[74] 专利代理机构 中国专利代理(香港)有限公司
代理人 吴立明 王忠忠

权利要求书 5 页 说明书 23 页 附图 13 页

[54] 发明名称 IP 通信传输的用户资源策略控制

[57] 摘要

公布了一个用来控制因特网协议(IP)通信传输的用户资源的方法，系统，以及计算机程序产品。在网络上跟踪端点组的网络利用可以产生与由端点组当前消耗的网络资源量相关的组利用级别信息。在组中的端点对数据流资源的请求可以从与该端点相关的路由器上接收。 对网络资源的请求包括一个与该端点相关的标识符。 决定是否接受请求是建立在组利用级别信息，标识符，以及与组相关的第一预定简档基础上，它包括一个第一网络利用限制。



ISSN1008-4274

1. 一种用来控制网络通讯量传输的用户资源的方法，包括：

在网络上跟踪端点的组的网络利用，以产生与当前被组利用的网络资源消耗量相对应的组利用级别信息；

接收一个与端点之一的数据流网络资源请求相应的消息，该请求包括一个与端点相关的标识符；以及

在组利用级别信息，标识符，以及预定简档的基础上决定是否接受请求，预定简档与组相关并包括一个网络利用限制。

2. 权利要求 1 中的方法，其中接收步骤包括：

从与端点相关的路由器和包交换器中的一个接收请求；以及

其中方法进一步包括步骤：

向路由器转发是否接受请求的决定结果。

3. 权利要求 2 的方法，其中路由器是一个策略执行点（PEP），而该方法进一步包括步骤：

从 PEP 接收一个端点数据流对网络资源的请求。

4. 权利要求 3 的方法，更进一步包括以下步骤：

在构成策略决定点的服务器上执行跟踪，接收，决定步骤。

5. 权利要求 1 的方法，其中决定步骤包括步骤：

应用策略规则，使用组利用级别的信息，标识符，以及预定简档决定组是否超过了网络利用限制。

6. 权利要求 5 的方法，其中在应用步骤中的规则包括：

访问控制规则，尝试率规则，带宽规则，最大并发数据流规则，以及数据流时间限制规则。

7. 权利要求 1 的方法，其中组是与保留带宽服务逻辑访问端口（RLAP）相关的，而该方法进一步包括：

跟踪 RLAP 的网络利用情况，RLAP 包括一个产生与被 RLAP 当前所消耗的网络资源量相关的 RLAP 利用级别信息的端点；并且

其中决定步骤包括：

在 RLAP 利用级别信息和其他与组相关的预定简档信息基础上决定是否接受请求，包括一个相应的网络利用限制。

8. 权利要求 1 的方法，进一步包括如下步骤：

当请求被接受时，调整组利用级别信息，以反映请求的安装以及相应网络资源消耗的增加。

9. 权利要求 8 的方法，进一步包括以下步骤：

接收另一个与数据流中断以及数据流以前消耗的网络资源有效性相关的消息；和

调整组利用级别信息以反映被数据流之前消耗的网络资源的有效性。

10. 一种用来控制网络通信传输的用户资源的系统，包括：

在网络上跟踪端点组的网络利用并产生与组当前消耗的网络资源相关的组利用级别信息的装置；

接收与端点数据流对网络资源的请求相关的消息的装置，该请求包括一个与端点相关的标识符；以及

在组利用级别信息，标识符，以及预定简档的基础上决定是否接收请求的装置，预定简档与组相关并包括一个组利用限制。

11. 权利要求 10 的系统，其中接收装置包括：

从与端点相关的路由器和包交换器中的一个接收请求的装置；并且

其中系统进一步包括：

将是否接受请求的决定结果转发给路由器的装置。

12. 权利要求 11 的系统，其中路由器包括：

一个策略执行点（PEP）；其中系统进一步包括

从 PEP 接收端点数据流对网络资源请求的装置。

13. 权利要求 12 的系统，进一步包括：

构成策略决定点的服务器，上述服务器包括跟踪的装置，接收的装置，以及作出决定的装置。

14. 权利要求 10 的系统，其中决定装置包括：

使应用策略规则的装置，用组利用级别信息，标识符，以及预定简档决定组是否超过了网络利用限制。

15. 权利要求 14 的系统，其中策略规则包括：

一个访问控制规则，一个尝试率规则，一个带宽规则，一个最大并发数据流规则，以及一个数据流时间限制规则。

16. 权利要求 10 的系统，其中组与保留带宽服务逻辑访问端口

应用策略规则，利用组利用级别信息，标识符，以及预定简档决定组是否超过了网络利用限制。

24. 权利要求 23 的计算机可读介质，其中应用步骤的策略规则包括:

一个访问控制规则，一个尝试率规则，一个带宽规则，一个最大并发数据流规则，一个数据流时间限制规则。

25. 权利要求 19 的计算机可读介质，其中组是与保留带宽服务逻辑访问端口（RLAP）相关的，计算机可读介质更进一步包括能够使计算机执行下列步骤的程序指令:

跟踪 RLAP 的网络利用，RLAP 包括产生与 RLAP 当前的网络资源消耗量相对应的 RLAP 利用级别信息的端点；和

其中决定步骤包括以下步骤:

在 RLAP 利用级别信息以及其他与包括相应网络利用限制组相关的预定简档的基础上决定是否接受请求。

26. 权利要求 19 的计算机可读介质，其中计算机可读介质更进一步包括可以使计算机执行下列步骤的程序指令:

当请求被接受的时候，调整组利用级别信息，以反映请求的安装以及网络资源消耗的相应增加。

27. 权利要求 26 的计算机可读介质，其中计算机可读介质更进一步包括能够使计算机执行如下步骤的程序指令:

接收另一个与数据流的中断相关以及与被数据流以前消耗的网络资源的有效性相关的消息；以及调整组利用级别信息以反映数据流先前消耗的网络资源的有效性。

28. 一种用来存储控制网络通信传输的用户资源的存储器，包括以下数据结构:

一个用来存储与策略执行点相关的第一标识符的字段;

一个用来与网络上的端点组相关的第二标识符的字段，端点组与策略执行点相联系；和

一个用来存储组的预定网络利用限制信息的字段。

29. 根据权利要求 28 的存储器，其中用来存储组利用限制信息的字段包括:

用来存储发生在某个具体时间段由组做出数据流请求的数目限制

的字段;

用来存储由组当前所使用的带宽量限制的字段;

用来存储组的当前有效的数据流数目限制的字段。

30. 用来存储网络通信传输的用户资源控制的信息的存储器，的数据结构包括:

一个用来存储关于策略执行点的第一标识符的字段;

一个用来存储关于网络上端点组的第二标识符，端点组与策略执行点相联系;

一个用来存储组的网络利用级别信息的字段，网络利用级别信息与组当前的网络资源消耗量相关。

31. 权利要求 30 的存储器，其中用来存储组利用级别信息的字段包括:

用来存储在某个具体时段由组做出的数据流请求尝试数目的字段;

用来存储组当前使用带宽数量的字段; 以及

存储组的当前有效的数据流数量的字段。

IP通信传输的用户资源策略控制

本发明一般涉及用户利用网络资源的控制，更具体地涉及用于跟踪用户在网络上的资源利用并加强了用户利用策略。

广域网（WAN），例如因特网，可以通过一个可能的网络把许许多多的计算机连接起来。因特网是使用 TCP/IP 协议组互相进行通信的网络和网关的集合。TCP/IP 协议和结构在 Liu 等人所著的“管理因特网信息服务”，O Reilly 和 Associates 公司，1994; Comer 所著的“TCP/IP 下的因特网第一卷：原理、协议、与体系结构”，Prentice-Hall 公司，1991; Comer 和 Stevens 所著的“TCP/IP 下的因特网第二卷：设计，实现，与内部网”，Prentice-Hall 公司，1991; Comer 和 Stevens 所著的“TCP/IP 下的因特网第三卷：客户机－服务器设计与应用”，Prentice－Hall 公司，1993 等等中有详细描述，所有这些资料都被结合在这里作为参考。

因特网的网关是提供因特网主干与其他网络之间连接的设备，例如用户的局域网（LAN）。因特网的网关通常面向的是计算机或者路由器。路由器是通信网络的中间设备，它可以接收传输信息并通过最有效的路径把它们传递给正确的接收端。一个因特网网关可以被看成因特网上的一个节点，通常可以执行数据转化，数据变换，信息处理，以及因特网主干和其他网络之间的协议转换。

主干是一个高速网络，它可以将局域性和区域内的网络连接在一起。一个内部链路包括至少一个能够与其他内部链路交换数据包的连接点。当今，许多商业网络供应商，例如 MCI Worldcom，都拥有其自己的采用微波中继和专用线的跨越数千英里的网络主干。

诸如因特网的计算机网络已经在信息传播重创建了分布广泛的效率。然而，通过因特网传输和接收数据的速度仍然有很大起伏。即使是在最大通信线路上数据流也可能会由于带宽限制而变得相当慢或者出现中断。随着诸如因特网的网络的商业和个人用途不断增加，带宽限制的问题变得越来越严重。

目前就带宽限制问题已经有多个解决方案被提出。其中一个解决

方案就是简单地提供一个带有额外带宽容量的网络。这个被称为额外提供的解决方案要求对网络提供更多的通信线路和/或带有额外带宽容量的通信线路。额外提供的代价是高昂的，并且会浪费带宽资源。此外，即使是额外提供的网络也可能在网络利用率超过网络带宽容量的时候出现供不应求的情况。

带宽限制问题的另外一种解决方案就是控制在每个路由器接口基础上的网络资源。换句话说，每个路由器都被给定了利用限制，而当超过这个利用限制的时候，路由器将不再接受数据流请求。近似的解决方案是使用 IETF（Internet 工程任务组）区别服务类。基于类别的资源控制在 Roberts 所著的“新型类别系统”，1977 年 10 月中进行了讨论，其网址是 http://www.data.com/roundups/class_system.html，这里将其作为参考在这里加以引用。

区别服务将包通信归类，并在不同类别的基础上提供服务性质。它是基于带有 DSCP（区别服务代码点）的包标记。数据包在路由器接口处根据 DSCP 被区别服务路由器分类，并且在每个区别服务路由器处接受为其 DSCP 配置的服务处理性质。

基于路由器接口的资源控制和基于服务类别的资源控制都是很粗糙的。特别是这些解决方案都要跟踪当前在每个路由器接口基础上或者只在每个类别基础上使用的资源。这些解决方案经常不能够防止网络资源被强度通信应用程序所消耗，这必将妨碍其他应用程序访问这些资源。

带宽限制问题的另一个解决方案就是每个会话信号机制中在 RSVP（资源保留安装协议）基础上控制网络资源。RSVP 是一个能够在网络路由器上运行的通信协议。RSVP 被设计用来一经要求就提供带宽。通过使用 RSVP 协议，远程接收者或者端点可以请求路由器为数据流保留特定的带宽量。路由器返回消息以指示该请求是否得到授权。这样一来，RSVP 可以提供一个在单个数据流基础上的获得网络资源准许的保留。然而，这个技术十分优秀。通常情况下，网络资源是基于每个数据流级别的微观管理，而不是在用户级别的管理。由于网络资源通常是在用户级别获得的，所以在每个数据流级别上的管理是不受欢迎的。

还有一种带宽限制问题的解决方案是在寻找传输和/或接收数据流

的端点 IP 地址基础上拒绝对网络资源访问。这个解决方案是非常粗糙的，然而它提供了资源分配的完全或者无用的途径。

因此，本发明的对象可以提供一个灵活的技术来控制和跟踪网络资源的分配和使用。

本发明的另一个对象可以在用户基础上控制网络资源的消耗。

根据本发明可以通过提供一个新颖的为网络通信传送控制用户资源的方法，系统，和计算机程序产品，以实现这些和其他一些目的。跟踪端点组的网络利用生成对应于当前端点组消耗的网络资源量的组利用级别信息。在组中的端点对数据流的网络资源的请求会在与该端点相关的路由器上被接收。对网络资源的请求包含一个与端点相对应的标识符。在组利用级别信息，标识符，以及与组相对应的第一规定协议子集以及包括第一网络利用限制的基础上做出是否接受请求的决定。

如果端点组是用户的话，那么本发明就使得跟踪用户的网络利用并在跟踪用户网络利用的基础上决定是否接受对用户分配网络资源的请求。更好的，是否接受来自用户的请求的决定是通过采用策略规则来决定是否组超过了一个或多个网络利用限制做出的。另外，端点可以被分为保留带宽服务逻辑访问端口（RLAP），它是由一个或多个组构成的。可以以与组相同的方式跟踪 RLAP 的网络利用，而是否接受保留网络资源请求的决定可以在组利用级别信息附加的 RLAP 利用级别信息的基础上做出。

当对网络资源的请求被接受，组利用级别信息和 RLAP 利用级别信息被更新，以反映与组和 RLAP 相应的网络利用的增长。依此类似，当数据流减小，利用级别信息被调整以反映相应 RLAP 和组对网络利用的减少。这样，就可以在用户级别对网络资源灵活地管理了。

可以在策略决定点跟踪网络利用，该点可以从路由器上接收保留带宽的请求。路由器最好是一个使用 IETF COPS（公共开放策略服务）－RSVP 的策略执行点（PEP）或者一个可以进行 COPS 的 RSVP 路由器。这样，本发明就被作为 RSVP 信号过程的扩展被实现。

对本发明更为完整的评价和许多伴随的相关优点可以在下面的具体详述中获得，其中伴随着相应的图示作为参考，从而使得能够更好

地理解本发明，其中：

图 1A 是一个计算机网络的示意图，在其中根据本发明的具体实施方案对用户资源进行控制；

图 1B 显示了图 1A 中的端点如何被传送到保留带宽服务逻辑访问端口（RLAP）和组中；

图 2 是一个访问控制记录的示意图，它可以存储与图 1B 中与访问 ID 相关的计算机网络相关的端点 IP 地址；

图 3 是一个访问简档记录的示意图，它可以存储与图 1B 中计算机网络端点相应的信息，它们带有各自的策略执行点（PEP）。，RLAP，和组；

图 4 是一个组简档记录的示意图，它可以存储与图 1B 中组之一的网络利用限制相关的信息；

图 5 是一个 RLAP 简档记录示意图，它可以存储与图 1B 中 RLAP 之一的网络利用限制相关的信息；

图 6 是一个数据流状态记录示意图，它可以存储关于当前图 1B 的计算机网络端点之间的数据流的信息；

图 7 是一个组利用记录的示意图，它可以存储图 1B 中组之一的网络利用级别信息；

图 8 是一个 RLAP 利用表单的示意图，它可以存储图 1B 中 RLAP 之一的 RLAP 利用级别信息；

图 9 是一个显示在图 1B 的计算机网络的两个端点之间如何使用 RAVP 信号建立数据流的示意图；

图 10 是一个显示如何使用 RSVP 信号中止两个端点之间的数据流的示意图；

图 11 是一个显示使用 RSVP 信号中止两个端点之间的数据流的另外一种方法的示意图；

图 12 和 13 是显示为 IP 通信传送实现用户资源策略控制的过程的流程图；

图 14 是一个显示在图 1B 的计算机网络上应用策略规则来控制用户资源的流程图；

图 15 是一个通用计算机系统的示意图，该系统可以被安排执行在图 1B 计算机网络中显示的一个或多个设备特殊用途的功能。

现在参考附图，其中相似的标号表示所有这些视图的相同或者相对应的部分，而具体到图 1A 来说，示意计算机网络 100 可以实现所说明的本发明。计算机网络 100 包括一个管理域 102；策略执行点（PEP）104，106，以及 108；策略决定点（PDP）110 和 112；规则数据库 114 和 116；以及端点 118，120，122，124，126，128，130，132，134，136，138，140，142，以及 144。处于参考的方便，附录 A 中提供了一个术语和缩写的术语表。

管理域 102 是一个处于相同管理控制下并出于管理目的被归类在一起的网络元件的集合。管理域 102 使用永久性的接线，例如电缆，和/或由电话，调制解调器，或者其他通信链接组成的临时接线，以允许借予不同计算机以及联接到管理域 102 上的其他设备之间的通信。管理域 102 可以包括计算机和由通信工具连接的相应设备。举例来说，管理域 102 可以是 vBNS（超高性能链路网络设备）保留带宽网络或者其他一些支持高性能，高带宽研究应用设备的全国性网络。另外，管理域 102 可以是任何链路网络（例如，因特网），因特网的一部分，包交换网络，或者其他任何的广域网（WAN）。

PEP 104，106 和 108 是策略执行所在的路由器或者包交换中心。这些策略决定与是否建立路径相关联。如这里所用的那样，“策略”是一个定义网络资源访问和使用标准的规则组合。路径是网络中两个节点之间的链接，举例来说，端点 118 和端点 144 之间的链接。端点使用 RSVP（资源保留安装协议）信号或者其他适当形式的信号，协议，或者通信语言发送 PEP 请求来建立路径。RSVP 信号在 1997 年 9 月 Braden，Zhang，Berson，Herzog，和 Jamin 等人所著的“资源保留协议（RSVP）”的一般功能说明，ftp://ftp.isi.edu/in-notes/rfc2205.txt 中有所描述，这里将它作为参考加以引用。PEP104，106 和 108 的 IP 地址显示了在图 1A 中所有相邻的 PEP。

PEP 104，106，108 最好是支持 COPS（通用开放策略服务）的 RSVP 路由器，通过编程可以使它在 RSVP 使用或者其他适用于执行策略决定的设备上行使基于策略的控制。支持 COPS 的 RSVP 路由器最好包括一个用来为进行例如管理控制，策略控制以及包分类，而对通信进行分类以及执行 RSVP 协议功能的邮件路由功能。策略控制 RSVP 功能使得

路由器作为一个策略执行点（PEP）来运行，它可以为了执行与特定数据流请求相关的策略服务器决定而使用 COPS 协议执行操作。

COPS 是一个查询和响应协议，它可以被用来在策略服务器（举例来说，PDP 112）和他的客户机（PEP 106，108）交换策略信息。COPS 协议的实例可以在 Boyle，Cohcn，Durham，Herzog，Rajan，和 Sastry1999 年 8 月 16 日在网络草拟的“COPS（通用开放策略服务）协议”，http://www.www.ietf.org/internet-drafts/draft-ietf-rap-cops-07.txt；以及 Boyle，Cohen，Durham，Herzog，Rajan 和 Sastry 在 1999 年 6 月 14 日网络草拟的“RSVP 的 COPS 利用”，http://www.ietf.org/internet-drafts/draft-ietf-rap-cops-rsvp.05.txt 中找到；以上两者都在这里加被作为参考加以引用。

PDP 110，112 是服务器，举例来说，DEC Alpha 服务器模型 DS10 或者其他一些合适的设备，例如可以在其上做出策略决定的计算机或者策略服务器。PDP 110 与 PEP 104 进行通信，而 PDP 112 则与 PEP 106 和 PEP 108 进行通信。最佳情况下，PDP 110 和 112 与 PEP 104，106，以及 108 使用 COPS 协议的同一个版本进行通信。

规则数据库 114 和 116 是存储器，举例来说，随机存储器（RAM），它可以存储用于限制对管理域 102 的访问的管理策略规则。管理策略规则被 PDP 利用来做出策略决定。规则数据库 114 和 116 可以是位于 PDP 110 和 112 的内部或者外部。

端点 118－144 是连接到管理域 102 的计算机。端点 118－144 被配置为通过管理域 102 发送和/或接收到其他端点的数据流。端点 118－144 可以通过调制解调器，拨号网络，高速电话线路，以及/或者任何其他适当的方法访问管理域 102。端点 118－144 通过一个或者多个路由器 104，106，和 108 连接到管理域 102 上。每个端点 118－144 的 IP 地址在它们的旁边显示出来。

图 1B 显示了计算机网络 110 的端点 118－144 如何能够被划分到 RBS 逻辑访问接口（RLAP）146，148，150，和 152 中。所有 RLAP 都与 PDP 110，112 中至少一个相对应。更进一步来讲，位于每个 RLAP 中的端点又被细分为组 154，156，158，160，162，164，以及 166。组 154 与 RLAP 146 和 PDP 110 相对应，组 156 与 RLAP 146 和 PDP110 相对应，组 158 与 RLAP 148 和 PDP 110 相对应，组 160 与 RLAP148 和

PDP110 相对应，组 162 与 RLAP150 和 PDP112 相对应，组 164 与 RLAP152 和 PDP112 相对应，组 166 与 RLAP152 和 PDP112 相对应。可以通过任何逻辑方式决定这些端点的 RLAP 和组的关系，举例来说，通过地理上的相近或者网络拓扑来决定。如果 RLAP 和/或组与用户相对应，那么就可以方便地在用户级别跟踪和管理网络资源了。

应该注意的是，由于用来实现本发明的硬件的多样化，对于拥有一定相关技术的专业人士来说，显然，图 1A 和 1B 的计算机网络 100 仅仅是以说明问题为目的的。为了实现这些变化，一个计算机（举例来说，图 15 的计算机 1500）可以被安排执行图 1A 和 1B 中的两个或者更多设备的特殊功能。举例来说，一个计算机可以被编程执行 PEP 和 PDP 的功能。另一方面，通过使用分布式处理技术，例如，两个或者两个以上编程计算机，可以被替换为图 1A 和 1B 中所示的任何一个设备。

此外，每个端点都可以与多个组和 RLAP 相对应。这种情况发生在端点被授权通过多个 PEP 访问管理域的时候。举例来说，如果端点 136 被授权通过 PEP106 和 PEP108 访问管理域 102，端点 136 将会在它通过 PEP 106 访问管理域的时候与组 162 和 RLAP150 相对应。另一方面，端点 136 会在通过 PEP 108 访问管理域的时候与组 166 和 RLAP152 相对应。

本发明可以存储与计算机网络上的端点，RLAP 和组的资源利用，RLAP 和组的简档数据，出现在管理域 102 上的数据流相关的信息。这个信息被存储于诸如硬盘，光盘，磁盘，和/或 RAM 的一个或多个存储器中。一个或多个数据库，例如规则数据库 114 和 116，可以存储用来实现本发明的信息。数据库是利用包含在例如硬盘，光盘，磁盘，和/或 RAM 的存储器中的数据结构（例如记录，表单，阵列，字段，和/或列表）组织起来的。

图 2 到图 8 描述了用来实现 IP 通信传输的用户资源策略控制的数据结构。这些数据结构被 PDP110 和 112 用来做出策略决定，它可以被 PEP104，106，和 108 来执行。图 2 到图 8 中显示的数据结构被存储于 PDP 110 和 112 各自的规则数据库 114 和 116，或者其他适当的存储设备中。存储于数据结构中的信息包括链接端点与其相应的 RLAP 和组的标识符以及 RLAP 和组的资源利用等级信息以及 RLAP 和组的预定简档

信息。

图 2 显示了一个访问控制记录 200，它包括存储端点地址前缀的字段 202，存储前缀位的字段 204，以及用来存储地址 ID 的字段 206。地址控制记录 200 可以存储被授权通过 PEP104，106，和 108 访问管理域 102 的所有端点。

端点地址前缀就是被授权访问管理域 102 发送数据流的端点的 IP 地址前缀。前缀位就是用来决定发送端是否被授权访问管理域 102 的 IP 地址前缀的主要位数。地址 ID 就是到每个端点地址前缀的所有 PEP 列表的链接，其发送端被授权访问管理域 102。起点就是对于从一个端点向另一个发送数据流的端点来说，管理域 102 的访问点。存储于特殊 PDP 的访问控制记录可以被归纳与一个访问控制表单内。

图 3 显示了一个访问简档记录 300。访问简档记录 300 可以存储所有访问 ID。多个访问简档记录可以被存储于单个访问简档表单内。访问简档记录 300 包括存储访问 ID 的字段 302，存储起始 PEP 的 IP 地址的字段 304，存储 RLAP ID 的字段 306，存储组 ID 的字段 308。PEP 的 IP 地址表明哪个 PEP 被授权与访问 ID 相应端点的流入点。RLAP ID 表示与该访问 ID 以及相应的端点相对应的 RLAP。举例来说，RLAP 146 与端点 118 相对应。组 ID 表示与该访问 ID 以及相应端点相对应的组。举例来说，端点 118 与组 154 相对应。

图 4 显示了组简档记录 400，它可以存储关于组 154，156，158，160，162，164，以及 166 之一的预定信息。预定信息包括组的最大网络利用级别信息。每个组都有其组简档记录 400，而组简档记录可以被一起存储于一个组简档表单中。组简档记录 400 包括存储过度分配因子的字段 402，存储组 ID 的字段 404，存储每个组尝试比率状况的字段 406，存储每个组最大尝试比率的字段 408，存储每个组带宽情况的字段 410，存储所有组流入令牌比率限制的字段 412，存储流入最大峰值的字段 414，存储出口令牌比率限制的字段 416，存储出口最大峰值的字段 418，存储数据流时间限制状态的字段 420，存储数据流时间限制的字段 422，存储最大并发数据流的字段 424。

组 ID 可以标识与组简档记录 400 相对应的组。尝试率状态标识尝试率规则（将在下面的图 14 中加以讨论）是否对于组来说是起作用的。最大尝试率就是组能够在给定时间段内尝试在管理域 102 上尝试开始

一个数据流的最大时间数。带宽状态表示带宽规则是否对组起作用。流入令牌率限制是最大流入令牌率，根据带宽，一个组可以向它请求数据流。出口最大峰值限制是最大出口峰值，根据带宽，就是允许现有数据流流出某个组的现有数据流的最大出口峰值。数据流时间限制状态表示数据流时间限制规则（将在下面关于图 14 的讨论中涉及）是否有效。数据流时间限制是流出一个组的数据流能够存在的最大时间数。另外，数据流时间限制可以使到一个组的数据流能够存在的最大时间数或者是进出组的数据流能够存在的最大时间数。最大平行流就是允许一个组中同时存在的数据流数。数据流的最大数可以分成入口数据流和出口数据流来分别监视。

图 5 说明了 RLAP 简档记录 500。每个 RLAP 都有一个 RLAP 简档记录，多个 RLAP 500 记录可被存储于一个 RLAP 简档表单内。RLAP 简档记录 500 包括一个存储过度分配因子的字段 502，存储 RLAP ID 的字段 504，存储尝试率状态的字段 506，存储最大尝试率的字段 508，存储带宽状态的字段 510，存储入口令牌率限制的字段 512，存储入口最大峰值的字段 514，存储出口令牌率限制的字段 516，存储出口最大峰值的字段 518，存储最大平行流的字段 520。存储于 RLAP 记录中的信息与存储于组简档记录 400 中的信息近似。举例来说，字段 508 中的最大尝试率就是 RLAP 能够尝试在管理域 102 上初始化数据流的最大时间数。

图 6 说明了数据流状态记录 600。数据流状态记录是为从一个端点（也就是发送端）穿过管理域 102 到另一个端点（也就是接收端）的每个数据流创建的。数据流状态记录 600 可以被全部存储于数据流状态表单中。数据流状态记录 600 包括存储 PEP 的 IP 地址的字段 602，存储客户端类型的字段 604，存储会话 ID 的字段 606，存储端点类型的字段 608，存储数据流计时器 ID 的字段 612，存储数据流计时器状态的字段 614，存储路径句柄的字段 620，存储保留句柄的字段 628，存储保留状态情况的字段 630，存储入口 RLAP ID 的字段 636，存储入口组 ID 的字段 638，存储出口 RLAP ID 的字段 640，存储出口组 ID 的字段 642，存储被数据流所使用带宽的字段 644。

PEP IP 地址就是数据流入口 PEP 的 IP 地址。客户类型可以确定 RSVP 客户的类型，（也就是说，使用 COPS/RSVP 协议的路由器）。会话 ID

可以确定会话。端点类型可以确定与 PEP 相对应的端点是否是一个未被确定的端点，入口端点，出口端点，或者一个混和入口和出口端点。数据流计时器 ID 可以确定与数据流状态记录 600 相对应的数据流计时器。数据流计时器可以跟踪与数据流状态记录 600 相关的数据流的持续时间。数据流计时器状态表示与数据流状态记录 600 相对应的数据流计时器是有效的还是无效的。路径句柄表示数据流的安装路径状态。保留句柄表示数据流的安装保留状态。

入口 RLAP ID 表示与入口处发送端相关的 RLAP。入口组 ID 表示与入口处发送端相关的组 ID。出口 RLAP ID 表示与出口处接收端相关的 RLAP。出口组 ID 表示与出口处接收端相关的 RLAP。举例来说，如果为数据流从端点 118 到端点 144 形成了一个正确的路径，PDP 110 就是出口 PDP，而 PDP 112 就是出口 PDP。依此类推，PEP104 就是出口 PEP，而 PEP 108 就是出口 PEP。

这里所使用的带宽就是数据流要求的经过分配，调整的带宽。这样一来，所使用的带宽就是数据流正在消耗的带宽资源的总量。带宽可以根据数据流以位每秒来计算。

图 7 说明了组利用记录 700，它可以存储与一个 PDP 相关组的网络利用（也就是资源消耗）的信息。每个与 PDP 相关组的组利用记录被存储于与 PDP（例如，与 PDP110 相对应的规则数据库 114）相对应的数据库中。每个组利用记录 700 都包括存储组 ID 的字段 704，存储最终行时间的字段 706，存储尝试的字段 708，存储所使用入口带宽的字段 710，存储所使用出口带宽的字段 712，存储有效数据流的字段 714。组 ID 可以确定组。最终行时间就是基于 ANSI 时间函数的最终行时间。最终行时间是由尝试率规则使用的，这将在下面关于图 14 的讨论中被涉及。最终行时间就是尝试数最后一次被重置的时间。尝试数就是数据流要求组在一定时间段内进行尝试的次数。时间段就是尝试每次被计数时的时间周期。尝试率在一定时间内进行尝试的数目。时间段是一个预先设定值，它通常被设置为 10 秒。所使用的入口带宽是组当前使用的合计出口带宽总量。另外可以看出来，对于每个组来说，入口带宽和出口带宽被分别追踪的，这样可以方便地允许带宽限制符合不通用户的要求。有效数据流是组中当前有效的数据流数目。

图 8 说明了 RLAP 利用记录 800，它可以存储与 PDP 相关的 RLAP

的网络资源消耗信息。与 PDP 相关的所有 RLAP 的 RLAP 利用记录 800 都被存储于与 PDP 相对应的数据库中（举例来说，在与 PDP110 相对应的规则数据库 114 中）。PDP 的 RLAP 利用记录可以被存储于一个表单中。RLAP 记录 800 包括存储 RLAP ID 的字段 804，存储最终行时间的字段 806，存储尝试的字段 808，存储所使用入口带宽的字段 810，存储所使用出口带宽的字段 812，存储有效数据流的字段 814。RLAP ID 可以确定与 RLAP 利用记录 800 相对应的 RLAP。最终行时间是基于 ANSI 时间函数的 RLAP 的最终行的时间。在应用尝试率规则以及与在组级别使用的最终行时间相近似的时候可以使用 RLAP 级别的最终行时间。尝试可以确定在预定取样时间里发生数据流请求尝试的数目。所使用的入口带宽 RLAP 当前使用的合计入口带宽。所使用出口带宽是 RLAP 当前使用的合计出口带宽。这样一来，RLAP 利用记录 800 与组利用记录 700 在出口带宽和入口带宽都被追踪方面是相似的。有效数据流可以确定当前对于 RLAP 有效的数据流数目。

图 9 是一个示意图，它说明了示范的消息交换以便建立从发送端到接收端的数据流。数据流的发送端和接收端分别是端点 118 和端点 144。图 9 中所显示的消息交换采用 RSVP 和 COPS 信号协议；PDP 用来实现本发明信息可以被封装到任何适当的消息内，然而还可以使用其他任何适当的协议。这样一来，如果 PDP 能够联系与它们的相关组和 RLAP 发送请求的端点并获得与数据流消耗和/或将要消耗网络资源总量相关的信息，任何协议语言，信号技术，或者其他任何通信方法都可以采用。

如图 9 中所示，PEP 104 和 108 是支持 COPS 的 RSVP 路由器。这样一来，PEP 104 和 108 使用 RSVP 信号协议分别与端点 118 和 144 进行通信，而 PEP 104 和 108 使用 RSVP 和 COPS 协议分别与 PDP 110 和 112 进行通信。

为了启动数据流，端点 118 利用一个 RSVP SENDER_TSPEC 对象发出一个路径请求（RSVP PATH），该对象为请求数据流描述了请求令牌率和峰值的通信特征。RSVP PATH 由 PEP 104 接收，而它就变成了入口访问点。PEP 104 向 PDP 110 发出一个 Request 消息类型的 PATH（REQ PATH）。PDP 110 可以确定该数据流是一个相对于 PDP 110，应用策略规则（将在关于图 14 的讨论中涉及），安装入口路径状态，并且没有

违反任何策略规则的话，向 PEP 104 返回一个决定命令来安装数据流（DEC 安装）的入口数据流。接下来，PEP 104 将 RSVP PATH 转寄给下游的 PEP 108，而后者在实例中是作为出口访问点的。在从 PEP 104 接收到 RSVP Path 之后，PEP 108 向 PDP112 发出 REQ PATH，而后再在本实例中是出口 PDP。PDP 112 决定数据流是一个关于 PDP 112 的出口数据流，应用策略规则，并安装出口路径状态。接着如果没有违反任何策略规则的话，PDP 112 将 DEC Install 返回给 PEP 108。然后，PEP 108 会将 RSVP PATH 向下游转寄给端点 144。如果确定 PDP 110 或者 PDP112 为反了策略规则的话，出现违反规则的 PDP 将不会向相应的 PEP 发出 DEC Install。实际上，PDP 将会向相应的 PEP 发出一个 DEC Remove，而随后，RSVP PATH 将不会被从该 PEP 转寄到别处。

假定 RSVP PATH 被成功地从端点 118 转寄到端点 144，端点 144 必须继续将 RSVP 保留消息（RSVP RESV）返回给端点 144 从而使数据流被初始化。端点 144 将 RSVP RESV 转寄给 PEP 108。RSVP RESV 可以确定诸如令牌率和峰值的通信特性。PEP 接收 RSVP RESV 并接着向 PDP 112 发出一个 Request 消息类型 RSVP（REQ RESV）。PDP 112 决定数据流是一个玉 PDP 112 相关的出口数据流，决定策略规则，为相应组和 RLAP 调整网络利用级别信息，然后安装保留指令。如果没有违反策略规则的话，PDP 112 将会向 PDP 108 返回 DEC Install。从 PDP 112 接收到 DEC Install 之后，PEP 108 通过向 PDP 112 发出报告提交（RPT Commit）来承认该决定，然后 PEP 108 将 RSVP RESV 转寄给 PEP 104。最后，PEP 112 更新或者调整与端点 144 相对应的 RLAP 152 和组 166 出口网络利用信息。接着，PEP 104 向 PDP 110 发送 REQ RESV，PDP 110 决定数据流是一个与 PDP 110 相关的入口数据流，应用策略规则，如果没有违反任何策略规则的话，为相应的 RLAP 146 和组 154 调整网络利用级别信息，并安装保留指令。然后，PDP 110 向 PEP 104 发送一个 DEC Install 并为与端点 118 相对应的 RLAP 146 和组 154 更新入口网络利用信息。依此类推，PEP 104 向 PDP 110 返回一个 RPT Commit，将 RSVP RESV 转寄给端点 118，于是就从端点 118 到端点 144 成功地建立了一个数据流。

图 10 和 11 是一个示意图，它说明了中止在图 9 中所建立的数据流的消息交换。图 10 说明了如何中止一个路径（也就是说，如何执行

中的特定用户相对应。

接下来，在步骤 210 中，对组和 RLAP 的网络利用的跟踪会产生组和 RLAP 利用级别的信息。组和 RLAP 利用级别分别与组和 RLAP 消耗的网络资源当前量相对应。组的网络利用是由使用存储在诸如组利用记录 700 的组利用记录中的信息跟踪的。依此类推，RLAP 的网络利用级别是由使用存储在诸如 RLAP 利用记录 800 的 RLAP 利用记录中的信息跟踪的。网络利用级别是随着 PDP 110 和 112 从 PEP 104 和 108 接收到表示数据流正在被创建或者终止的消息而被调整的。

在步骤 1220 中，PDP（例如 PDP 110）接收到一个为数据流对网络资源的请求（例如对保留带宽的请求）。这个请求最好是从一个 PEP（例如 PEP 104）上被接受，它是与 RLAP 146 以及组 154 和 156 相对应的，但是也可以从任何可以发出数据流请求的设备上接收。

于是，在步骤 1230 中，PDP 110 通过应用至少一条策略规则来决定对网络资源的请求是否可以被接受。策略规则是在存储于对应组利用记录 700 和 RLAP 利用记录 800 中的组和 RLAP 利用级别信息的基础上加以应用的，确定与发出请求（例如从访问简档记录 300 中获得）端点相关的组和 RLAP，以及对存储于相应组简档记录 400 和 RLAP 简档记录 500 中的相应组和 RLAP 的预测简档。

接下来在步骤 1240 中，PDP 110 通知 PEP 104 决定是否对发送端对网络资源的请求授权。

假设对网络资源和建立数据流的请求被 PDP 110 接受，组和 RLAP 利用级别就会被根据请求的接受情况以及在步骤 1300 中相应组和 RLAP 的有效带宽减少情况进行调整，具体如图 13 所示。一旦数据流被终止，PDP 110 就会在步骤 1310 中接受与终止数据流相应的请求。然后，在步骤 1320 中，PDP 根据对 RLAP 和组有效的网络资源的增加而调整组和 RLAP 的利用级别。

图 14 是一个说明策略规则如何被应用到图 12 的步骤 1230 中的流程图。在步骤 1400 中，应用访问控制规则可以确定发出请求的端点是否被授权网络入口和/或出口并确定那个组和 RLAP 简档记录是与端点相对应的。由于端点地址前缀被发送给与产生请求的 PEP 相应的 PDP，所以这些都是可行的。PDP 检查它的访问控制记录以确定是否有访问控制记录（举例来说，访问控制记录 200）拥有与发出请求的端点相

路径拆卸）。RSVP PathTear 消息是由端点 118 初始化的。RSVP PATHTear 消息还可以通过路由器来进行初始化，诸如 PEP 104 和 108 中的一个。PEP 104 从端点 118 接收到 RSVP PATHTear 请求。PEP 104 将 RSVP PATHTear 消息转寄给 PEP 108。PEP 108 将 RSVP PATHTear 转寄给端点 144。当 RSVP PATHTear 在 PEP 104 上被接收到的时候，会从 PEP 104 向 PEP 110 发送一个删除相应路径的请求指令（DRQ）。PDP 根据接收到的 DRQ 删除相应的状态。依此类推，当 PEP 108 从 PEP 104 接收到 RSVP PathTear 消息的时候，PEP 108 向 PDP 112 发出一个 DRQ。与所使用的结构和/或具体协议无关，拆卸可以被用来初始化网络利用级别的调整。

图 11 是一个示意图，它说明了包括在一个保留状态的成功拆卸之中的示范性消息交换。端点 144 将一个 RSVP ResvTear 消息初始化，该消息是被发送到 PEP 108 的。另外，还可以通过诸如 PEP 104 或者 PEP 108 的 RSVP 路由器初始化 RSVP ResvTear 消息。根据从端点 144 接收到的 RSVP ResvTear 消息，PEP 108 将 RSVP ResvTear 消息转寄给 PEP 104 并向 PDP 112 发出一个 DRQ。根据从 PEP 108 接收到的 RSVP ResvTear 消息，PEP 104 将 RSVP ResvTear 消息转寄给端点 118 并向 PDP 110 发出一个 DRQ。根据接收到的 DRQ，PDP 110 和 112 删除相关的保留状态。

当 PDP 110 和 112 接收到 DRQ 请求的时候，PDP 110 和 112 味相应的 RLAP 和组调整了网络利用级别信息以反映网络资源有效性的增加。通过这种方式，可以跟踪和更新组和 RLAP 利用表单。要想建立成功的路径，可以采用任何适当的协议语言来终止端点 118 和 144 之间的数据流。在 PDP 110 和 112 接收到表示数据流已经被终止的消息时，PDP 110 和 112 就可以更新，并从而跟踪，RLAP 和组的网络利用级别。

图 12 和 13 是描述实现 IP 通信传送的用户资源策略控制的流程图。在步骤 1200 中，计算机网络 100 的端点 118－144 被划分成 RLAP 146，148，150 和 152。RLAP 146 被分成组 154 和 156。RLAP 148 被分成组 158 和 160。RLAP 150 构成了一个单独的组 162。RLAP 152 被分成组 166 和 164。最佳情况下，RLAP 中的分组和组是合理的。此外，组和 RLAP 并不需要被网络的物理拓扑所约束。举例来说，组可以与位于同一建筑或者城市内的诸多端点相对应，而 RLAP 可以与管理域 102

匹配的端点地址前缀。每个访问控制记录都包括前缀位信息，它表示端点 IP 地址与存储在访问控制记录中的端点地址前缀相比较的重要位数。如果出现匹配，（也就是说，如果存在与发出请求的端点的访问记录 200），那么就会从端点的访问控制记录 200 之中获得访问 ID。访问 ID 被用来找到相对应的访问简档记录（举例来说，访问简档记录 300）。当访问简档记录中有访问控制记录中一样的访问 ID 时，产生请求的 PEP 的 IP 地址（也就是出口 PEP 的 IP 地址）被用来决定与发出请求的端点相对应的 RLAP 的 ID 以及组 ID。由于出口 PEP 的 IP 地址被链接到访问简档记录中相应的 RLAP ID 和组 ID 上，所以这些都是可行的。如果发送请求的端点尚未被授权，可以测试接收端端点的 IP 地址以确定是否存在与端点 IP 地址相对应的访问控制记录。如果找到产生请求 PEP 的 IP 地址和接收端地址的访问控制记录 200，也就是说，出口 PEP 的 IP 地址（在接收端端点的访问简档记录中列出），访问控制规则就没有被违反。如果发送端没有访问控制记录，或者发送端和接收端都拥有访问控制记录但是两者都没有带有与产生请求的 PEP 的 PEP IP 地址相匹配的出口 PEP IP 地址的访问简档记录，那么就会出现访问控制规则被违反或者出错。

当访问控制规则出错的时候，请求会被拒绝而不必再近一步测试规则。访问控制记录的一个特性就是 PDP 正在服务的 PEP 可以被决定。这个信息被用于策略规则的后继应用程序，它是依赖于相应 PEP，RLAP，和/或组的确定的。通过使用前缀位信息，端点地址前缀，以及访问控制记录，最长前缀，匹配可以被用来发现与发送端相关的访问控制记录。更进一步来讲，PDP 可以在应用访问控制规则其间确定它是否为一个入口访问点或者出口访问点。特别是，如果发送端拥有一个访问控制记录并且产生请求的 PEP 作为入口 PEP IP 地址被列在与发送端相关的访问简档记录中，那么该 PDP 就是一个入口访问点。在下列情况下该 PDP 是一个出口访问点：（1）它不是入口访问电，（2）接收端带有一个访问控制记录，以及（3）产生请求的 PEP 拥有列在接收端的访问简档记录中的 IP 地址。PDP 还可以为特殊的请求作为入口访问点和出口访问点。

在图 14 的步骤 1410 中，这里应用了一个尝试率规则。尝试率规则是被新路径请求所调用的。PDP 分别确定 RLAP 和组简档记录 500 和

400 中的最大尝试率。如上所述，在应用访问控制规则其间，可以确定适当的 RLAP 和组。可以使用一种定量视算法，这可以使得不需要持续监视尝试数目了。定量窗算法是在处理尝试率特性过程中内部应用的一个算法。在每个行时间间隔之间，计数器会随着分别为组和 RLAP 定义的尝试值的变化而更新。尝试率特性每被执行一次，当前时间与最终行时间之间的差异都会被与所设置的尝试率时间周期相比较。如果这个差值小于尝试率时间间隔，那么计数器递减，否则计数器会随着预定的尝试数更新，并且最终行时间会随着当前时间的变化而更新。如果没有超过最大尝试率的话，请求就会通过尝试率规则，否则的话，就违反了尝试率规则并且尝试失败。尝试率规则会被首先应用于 RLAP，然后是组。然而，这个顺序可以随着要求而变化。

另外，组和 RLAP 的路径请求尝试可以被分别跟踪并分别存储于相应的组利用记录以及 RLAP 利用记录中。如果存储于组利用记录中的尝试数超过存储于组简档记录中的最大尝试率的话，就违反了尝试率规则。依此类推，如果存储于 RLAP 利用记录中的尝试数超过 RLAP 简档记录中的最大尝试率，也违反了尝试率规则。全部被存储于 RLAP 利用记录和组利用记录中尝试数可以被定期重置，这可以使得自上次重置之后每经过由时间长度定义的预定时间量，尝试就表示尝试数。

在步骤 1420 中，应用带宽规则可以确定接受路径请求或者保留请求是否会导致超过组和 RLAP 的可允许最大带宽。带宽规则是为了响应路径请求和保留请求而被调用的。通过这种方式，可以对相对应入口和出口数据流的带宽分别监视。不同的带宽规则可以分别应用或者以所希望的结合方式以及顺序应用。第一带宽规则决定数据流的请求的通信特性超过相应的组简档记录 400 和 RLAP 简档记录 500 预定限制(也就是说，入口令牌率限制或者出口令牌率限制，这依赖于 PDP 是否是一个入口或者出口访问点）。这种检验可以在一个独立的数据流请求级别上执行，也可以在 RLAP 和组的合计带宽利用级别上执行。发送端的 RLAP 和组简档记录在入口点被用作带宽检查，而接收端的 RLAP 和组简档记录在出口点被用作带宽检查。请求的带宽数据通信参数（例如，峰值和令牌率）会被与组和 RLAP 的预定限制值相比较，这些预定值都被分别存储于相应的组利用记录和 RLAP 利用记录中。如果超过了 RLAP 限制值的话，请求失败而不再应用其他规则。依此类推，如果组

限制值被超过的话，请求失败并且也不再应用其他规则。

如果通信数据参数没有超过对于单独路径请求的限制值，就会对被 RLAP 使用的合计带宽进行估算。调整的带宽请求是由将入口令牌率限制（或者如果 PDP 是一个出口访问点的话，就衡量出口令牌率限制）与能够潜在影响有效带宽的附加带宽数量相衡量而决定的。调整带宽是令牌率限制和有利的峰值的总和。有利峰值就是令牌率限制和峰值限制之间的差值乘以峰值与剩余未被分配带宽的比率，当峰值限制小于等于令牌限制的时候，令牌率限制被用于调整带宽请求。这样一来，调整带宽请求的公式就是如下所示：

ABR=TR+[(PR-TR)*(PR/UB)]，

其中 ABA 就是调整带宽请求，TR 是令牌率，PR 是峰值，而 UB 是未被分配的贷款。

未被分配的带宽（UB）就是最大带宽与正在使用带宽之间的差值。有效带宽等于未被分配带宽乘以过度分配因数。过度分配因数就是允许网络管理员通过考虑到实际数据流中未获准的请求并通过授权请求使得带宽“过度分配”而优化网络资源控制的值。过度分配近似于某个班机被过度登记预定的定期航线。举例来说，当网络管理员认为，通过对利用情况的分析表明 10%用户对带宽的请求不会导致实际数据流，而管理员将为用户组配置一个 1.1 的过度分配因数。一旦被使用，过度分配因数可以被存储于，举例来说，字段 402 和 502 的组和 RLAP 简档记录中。有效带宽会与调整带宽请求相比较，如果调整带宽请求并没有超过过度分配的有效值的话，不会应用带宽规则。调整带宽请求被作为带宽使用信息的一部分存储于字段 644 的一个数据流状态记录中（举例来说，数据流状态记录 600）。另外，依赖于数据流是入口还是出口，调整带宽请求加上 RLAP 使用的合计带宽，它被存储于字段 810 或者字段 812 中的 RLAP 利用记录(举例来说,RLAP 利用记录 800)中。在访问控制期间可以确定数据流的类型（也就是入口和出口），它在成功完成保留请求的时候被存储于数据流状态记录的字段 608 中。

如果通信数据参数没有超过 RLAP 上面的限制状态的话，可以对组所使用的合计带宽进行估计。组合计带宽是以与 RLAP 合计带宽相似的方式利用组简档和利用记录，而不是 RLAP 简档和利用文件计算的。不

管带宽特性是否是被授权的且是有效的，调整带宽请求是与数据流状态信息（字段 644 中使用的带宽）存储在一起。而在确定所使用的合计带宽中需要解决调整带宽请求。

发送端和接收端的简档和利用信息涉及 RLAP 和组级别的带宽处理。与发送端相关的简档和利用数据是用来在入口点进行入口带宽计算的。与接收端相关的简档利用数据是用来在出口点进行出口带宽计算的。

在成功完成保留请求的基础上，RLAP 和组利用的合计带宽会被调整。请求的带宽被添加到入口点的发送端 RLAP 和组利用数据的合计数据中。请求带宽被添加到出口点的接收端 RLAP 和组利用数据的合计数据中。需要为现有保留量更改资源需求的后继请求被反映到这个合计数据中。

当数据流被终止（举例来说，当从 PDP 接收到一个 BRQ 的时候），与数据流相关的个别带宽被从 RLAP 和组的带宽合计量中扣除。入口合计带宽是与数据流发送端相对应的值。出口合计带宽就是与接收端相对应的值。如果请求带宽超过入口点的最大入口带宽或者超过出口点的最大出口带宽的话，就会违反带宽规则并导致请求失败。

在步骤 1430 中调用了最大并发数据流规则。这些规则可以对路径请求和/或保留请求的响应而被调用。PDP 确定接收请求数据流是否会导致并发数据流的最大数值超过 RLAP 和组的数值。通过比较存储于 RLAP 和组利用记录中的有效数据流数目信息和存储于 RLAP 和组简档记录中的最大并发数据流限制相关信息，上面的操作就得以执行。在最佳情况下，最大并发数据流规则在被用于组之前先被应用于 RLAP；然而，也可以采取其他的顺序应用。最大并发数据流规则是在发送端的组简档记录（例如，组简档记录 400），RLAP 简档记录（例如，RLAP 简档记录 500），组利用记录（例如，组利用记录 700），RLAP 利用记录（例如，RLAP 利用记录 800）的基础上应用的。如果没有违反最大并发数据流规则的话，在相应的组和 RLAP 利用记录中的有效并发数据流数会被增加，以反映资源消耗的增加。不惯最大并发数据流规则是否被授权并且是有效的，最好为成功的保留请求增加有效并发数据流数。当路径被终止并且 PDP 接收到一个 DRQ，组和 RLAP 利用记录的有效并发数据流数都会被扣除以反应资源消耗的减少。

在图 14 的步骤 1440 中，应用数据流时间限制规则可以确定现有数据流的最大允许数据流时间是否超过组的数据流时间限制。另外，应用数据流时间限制规则还可以应用于 RLAP 或者同时应用于组和 RLAP。在确定一个成功的保留请求的基础上可以调用数据流时间限制规则。更改保留带宽的后继请求不会重置或者影响数据流的计时器。依此类推，一个后继保留错误请求并不会重置或者影响数据流的计时器。在存在期间，数据流被入口 PDP 定期监视以确定它的持续时间已经超过了与发送端相关的存储于组简档记录中的预定数据流时间限制。如果数据流在超过时间限制的一段时间之内是有效的，入口 PDP 将数据流状态更改为“过期”并发出一个自动决定消息指示相应的 PEP 删除数据流。

因此，可以理解，本发明了一个 IP 通信传输的用户资源策略控制。策略规则是基于每个用户实现的，这如同在计算机网络的组和 RLAP 中定义的一样。

在上面提出的大多数实例中，本发明都根据使用 COPS 和 RSVP 协议的 IETF 结构描述的。然而，任何适当的协议都可以与 COPS 和/或 RSVP 协议一起使用，或者代替它。更进一步来讲，本发明或者其中一小部分可以使用常规通用计算机或者是根据本发明教学为目的设计的微处理器来实现，而这对于那些计算机专业人士来说这些都是显而易见的。适当的软件是为那些根据公布方案所教授的内容具有普通技术的人员设计的，这对于那些软件专业人士来说是游刃有余的。

图 15 是一个用来实现本发明方法的计算机系统 1500 的示意图。计算机系统 1500 包括一个用来覆盖插件板 1504 的计算机外壳 1502，它包含一个 CPU 1506，一个存储器 1508（例如随机存储器（RAM），动态 RAM（DRAM），静态 RAM（SRAM），同步 DRAM（SDRAM），闪烁 RAM，只读存储器（ROM），可编程存储器（PROM），可擦写 PROM（EPROM），以及电可擦除 PROM（EEPROM）），以及其他任选特殊作用的逻辑器件（例如，特定用途集成电路（ASIC））或者可配置逻辑器件（例如通用逻辑阵列（GAL）或者可重复编程域可编程门阵列（FPGA））。计算机系统 1500 还包括多种输入方式，例如键盘 1522 和鼠标 1524，以及用来控制监视器 1520 的显示卡 1510。另外，计算机系统 1500 进一步包括一个磁盘驱动器 1514；其他可移动介质驱动器（例如，光盘 1519，

磁带，可移动磁光介质）；以及硬盘 1512，或者其他混合型，高密度介质驱动器，它们都是通过合适的设备总线（例如，小型计算机系统接口（SCSI）总线，和增强型集成设备组建（IDE）总线，或者一个超直接存储器存取（DMA）总线）。计算机系统 1500 可以另外包括一个光盘阅读器 1518，一个法光盘读写单元，或者一个光盘自动唱机，所有这些都可以链接到相同的设备总线或者其他设备总线上。尽管光盘 1519 在图中是位于光盘盒中，但是它可以被直接插入 CD-ROM 设备中，而它并不需要光盘盒。另外打印机可以提供图 2-8 中所示的数据或者其他由计算机系统 1500 存储和/或产生的数据的结构列表。

如上面所说，系统包括至少一个计算机可读取介质或者根据本发明编程的存储器，他用来包括数据结构，表单，记录，或者这里所描述的其他数据。计算机可读取介质的实例包括光盘，硬盘，软盘，磁带，磁光盘，PROM（EPROM，EEPROM，闪烁 EPROM），DRAM，SRAM，SDRAM 等等。本发明还包括控制计算机 1500 硬件并使其能够与个人用户（消费者）进行交互的软件，它们都被存储在一个或者混合型的计算机可读介质中。这些软件可以包括设备驱动程序，操作系统和用户应用程序，例如开发工具等等，但是它并不仅仅限于此。这种计算机可读取介质更进一步来说还包括，本发明用来为实现本发明而执行全部处理过程或者其中一部分（如果处理过程是分布式的）的计算机程序产品。本发明的计算机编码设备可以是任何可解释的或者是可执行的编码机制，包括但是并不限于教本，解释程序，动态链接程序库，Java 类，以及完整的可执行程序。更进一步来讲，本发明的一部分处理过程可用于得到更佳的性能，更牢固的可靠性以及更低的价格。

本发明还可以通过配备特殊集成电路应用程序或者通过将常规组件电路的互联成适当的网络来实现，这对于专业人士来说是相当容易理解的。

显然，根据上面的教授中，本发明还可以存在大量的修改方案以及演变。因此需要理解的是，在附加的权利要求中，本发明可以如这里所具体讲述的一样通过不同的方式来实现。

附录 A 术语和缩写的词汇表

访问点－访问点就是数据流流进或者流出管理域的点。

地址前缀－地址前缀 Ipv4 地址或者 Ipv6 地址的开头部分，加上

一个定义在最大匹配比较中使用的首项数目的整数。地址前缀并不与组交迭。

DEC Install－DEC Install 是一个表示请求被授权的 COPS 判定操作。它会导致安装与请求相关数据流的 PEP 指令。

DEC Remove－DEC Remove 是一个表示请求被拒绝的 COPS 判定操作。PEP 并不为与请求相关的数据流安装指令。

Decision－Decision 是在管理规则基础上从 PDP 发送到 PEP 的一个响应。

DRQ－删除请求指令。DRQ 是一个 COPS 操作，其中 PEP 向 PDP 发送 DRQ 表示与该请求相关的状态将被删除。在拆卸的情况下才会发送 BRQ。

Egress－出口是一个发送端的出口，或者是管理域的离去点。由于 RSVP 是单向性的，所以出口点总是站在发送端角度来说的；然而，发送端的出口点将会是接收端的入口点。

出口带宽－出口带宽就是由数据流的接收端所利用的带宽。

端点－端点就是 RSVP 主机发送端或者接收端并被指派了一个 IPv4 或者 IPv6 地址。端点可以通过多路由器访问网络。

数据流－数据流就是介于发送端和接收端之间的特殊数据流。

出口带宽－出口带宽就是由数据流发送端利用的带宽。

组－组就是共享在 Group Profile 指定的相同规则的端点集合。多个组可以被指定在一个 RLAP 里。组可以由一个或者多个成员组成。

入口－入口就是发送端入口，或者进入管理域的访问点。由于 RSVP 是单向的，所以入口点总是站在发送端的角度来说的；然而，发送端入口电将会是接收端的出口点。

路径－路径就是为了请求保留由发送端向接收端发送 RSVP 操作。它采用保留的数据流所采用的路由器。

峰值－峰值就是每秒所传输的连续的，不间断的位数。这样，峰值就是实时位数值或者是一个相关近似值。

策略－策略就是策略和服务的集合，其中规则定义了资源访问和利用的标准。

PEP－策略执行点。PEP 就是策略决定被实际执行的地方。

PDP－策略决定点，PDP 就是做出策略决定的地方。

RBS－保留带宽服务。RBS 是一个利用管理策略规则来限制对管理域的访问的服务。

报告－报告就是从 PEP 向 PDP 发送的一个消息，它向 PDP 通报 PEP 的情况。

请求－请求就是从 PEP 向 PDP 发送的一个消息，它为 RSVP 数据流发出一些请求。

保留－保留就是由接收端向发送端发出的一个 RSVP 操作，它可以保留介于接收端和发送端之间的路径每个节点处的网络资源。

REQ PATH－REQ PATH 就是由 PEP 向 PDP 发送的 COPS 操作，它可以做出包括 RSVP PATH 消息信息的策略请求。

REQ RESV－REQ RESV 就是由 PEP 向 PDP 发送的 COPS 操作，它可以做出包括 RSVP Reservation 消息信息的策略请求。

RESV STATE－RESV STATE 就是与 RSVP 数据流的保存相关的状态。保留状态与 RSVP 要求的网络资源的分配相关。

RLAP－RBS 逻辑访问端口。一个 RLAP 就是 IPv4 和 IPv6 地址的逻辑分组。多个 RLAP 可以被指定一个 PEP。RLAP 地址分组可以应用于一个 PEP。最佳情况下，RLAP 中的所有端点可以通过相同的 PEP 访问管理域。

RPT 提交－RPT 提交是 PEP 发送给 PDP 的一个 COPS 操作，它可以识别关于前面由 PDP 向 PEP 发送的 DEC Install 相关的状态信息。

RSVP－资源保留协议。

RSVP PATH－RSVP PATH 是有发送端向接收端发送的请求为建立的路径保留带宽的 RSVP 操作。

RSVP PATHTEAR－RSVP PATHTEAR 是由发送端向接收端发送的指示数据流被终止的 RSVP 操作。

RSVP RESVTEAR－RSVP RESVTEAR 是由接收端向发送端发送的只是数据流被终止的 RSVP 操作。

Session－一个对话就是带有特定目的地喝传输层协议的数据流（例如，一个 RSVP 数据流）。它是由 5 个元素定义的（DestAddress，ProtocolId，DesPort，SrcAddress，SrcProt）。

State－State 就是明确到一个实体（例如，一个数据流）的信息，它反映了一个时期或者阶段。

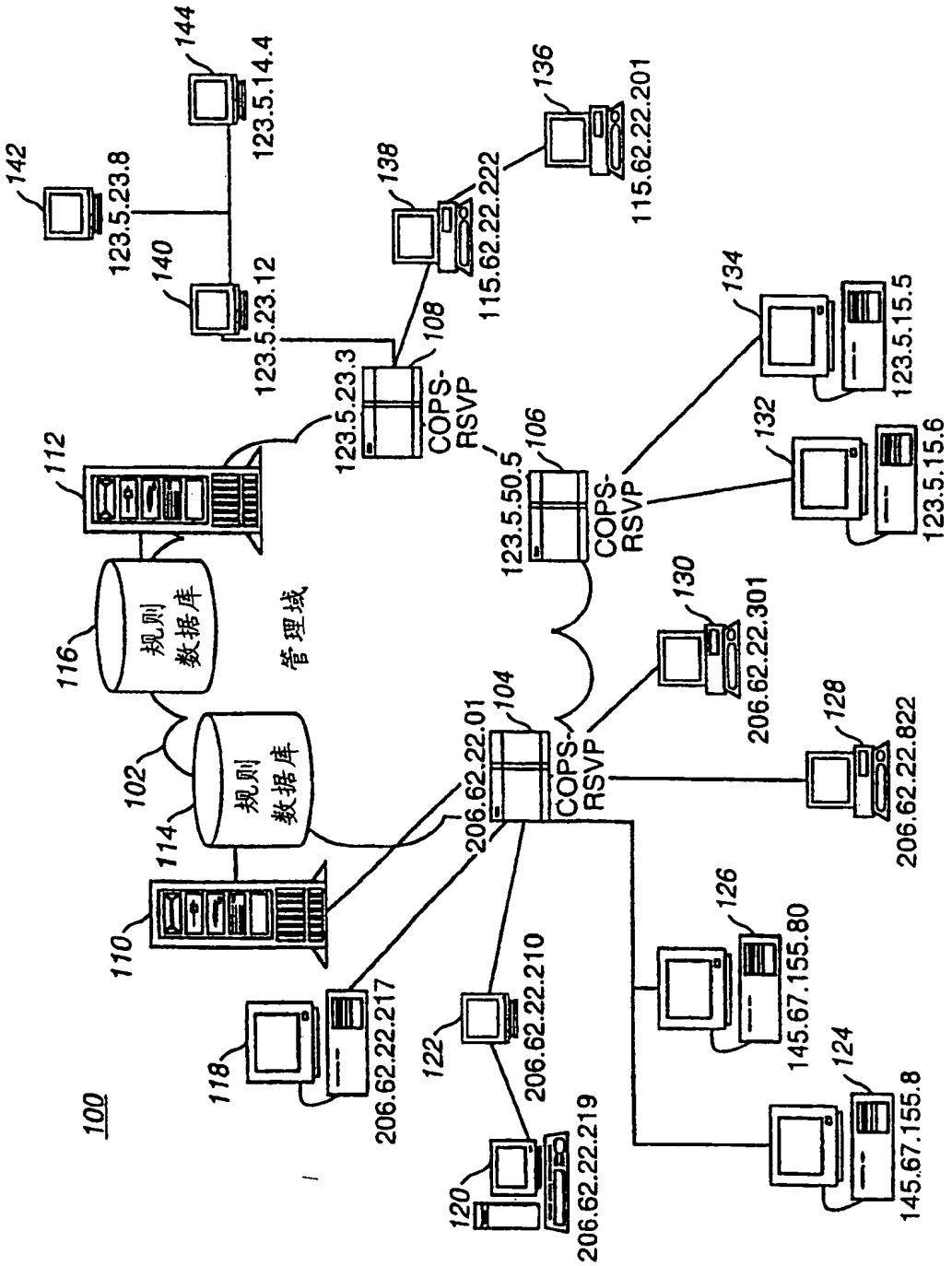

100
142
123.5.23.8
144
123.5.14.4
140
123.5.23.12
138
115.62.22.222
136
115.62.22.201
108
123.5.23.3
COPS-RSVP
112
106
123.5.50.5
COPS-RSVP
134
123.5.15.5
132
123.5.15.6
116
规则数据库
管理域
130
206.62.22.301
102
114
规则数据库
104
206.62.22.01
COPS-RSVP
128
206.62.22.822
110
126
145.67.155.80
118
206.62.22.217
122
206.62.22.210
124
145.67.155.8
120
206.62.22.219

图 1A

Token Rate－Token rate 是每秒所传输的持续不便的位数。这样一来，令牌率就是平均位数值。

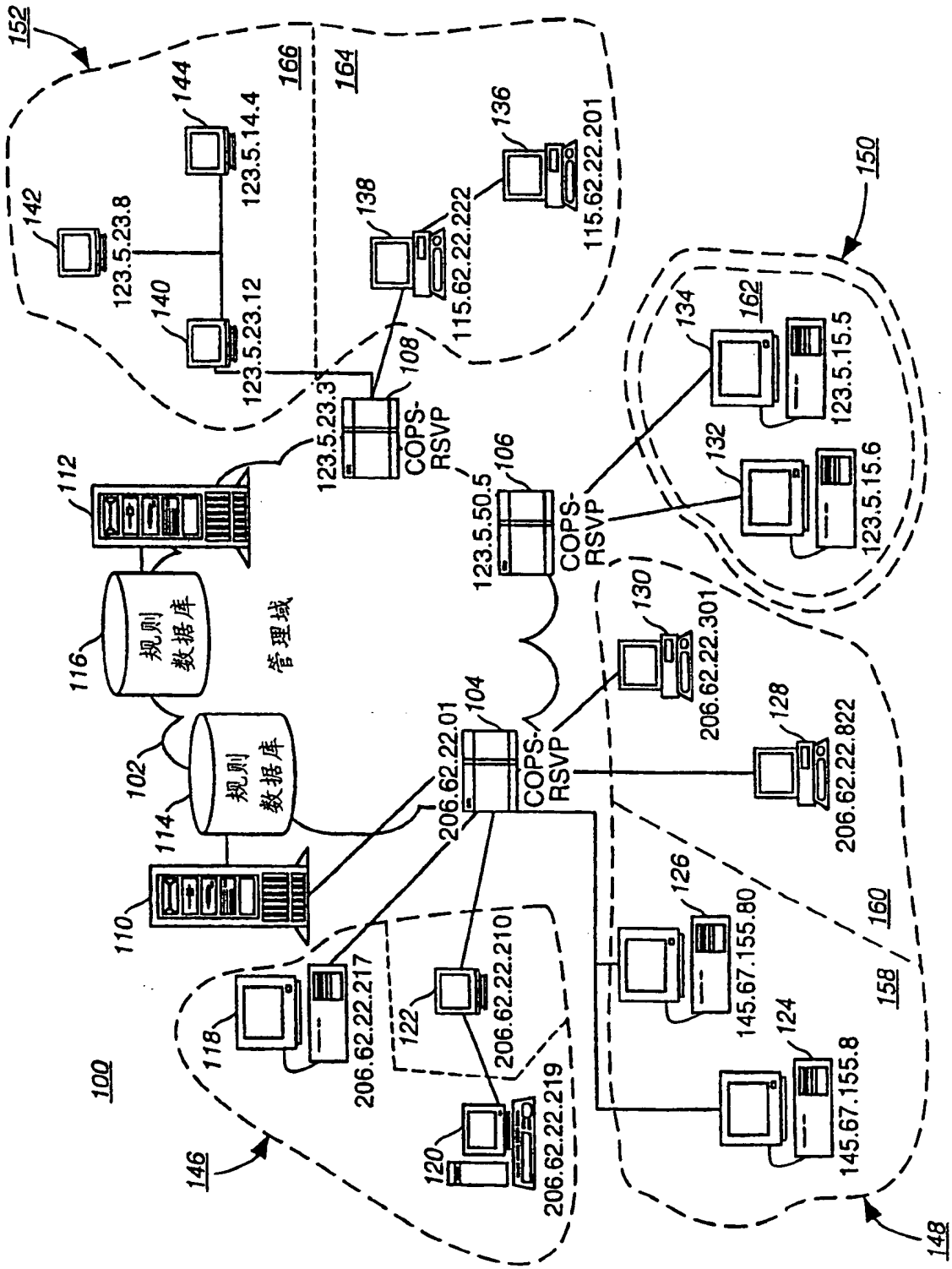

152
166
164
144
123.5.14.4
142
123.5.23.8
140
123.5.23.12
138
136
115.62.22.222
115.62.22.201
108
123.5.23.3
COPS-RSVP
106
123.5.50.5
COPS-RSVP
150
162
134
123.5.15.5
132
123.5.15.6
112
116
规则数据库
管理域
102
规则数据库
114
110
104
206.62.22.01
COPS-RSVP
130
206.62.22.301
128
206.62.22.822
126
145.67.155.80
160
158
124
145.67.155.8
118
206.62.22.217
122
206.62.22.210
120
206.62.22.219
146
100
148

图 1B

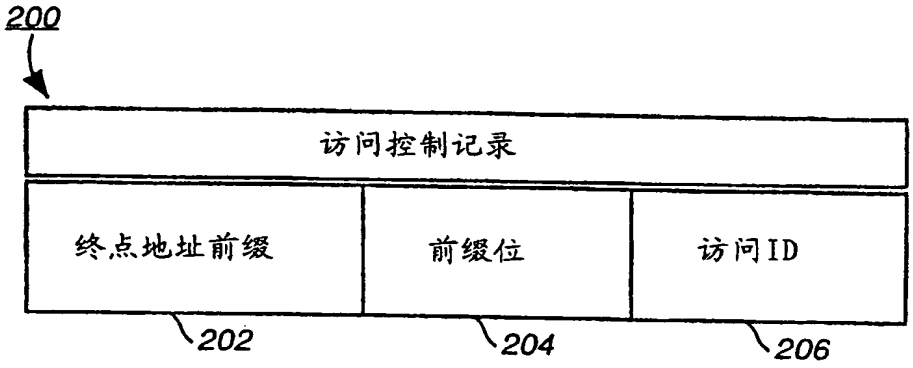

200
访问控制记录
终点地址前缀
前缀位
访问ID
202
204
206

图 2

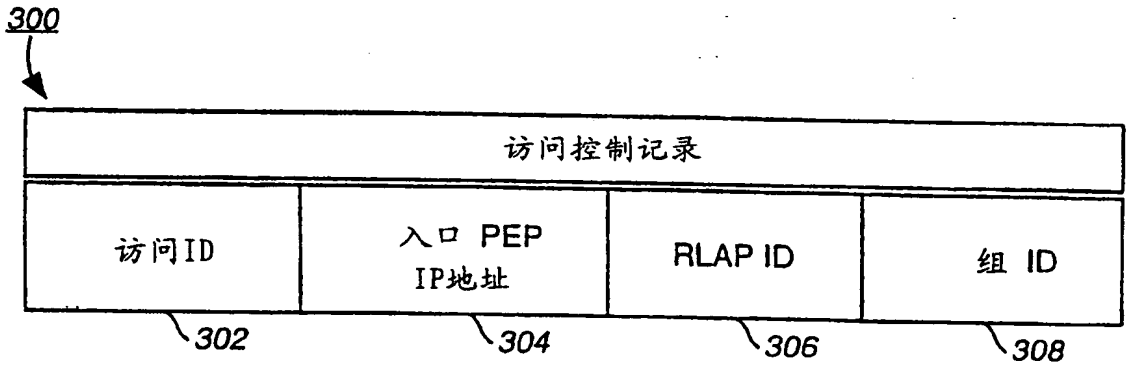

300
访问控制记录
访问ID
入口 PEP
IP地址
RLAP ID
组 ID
302
304
306
308

图 3

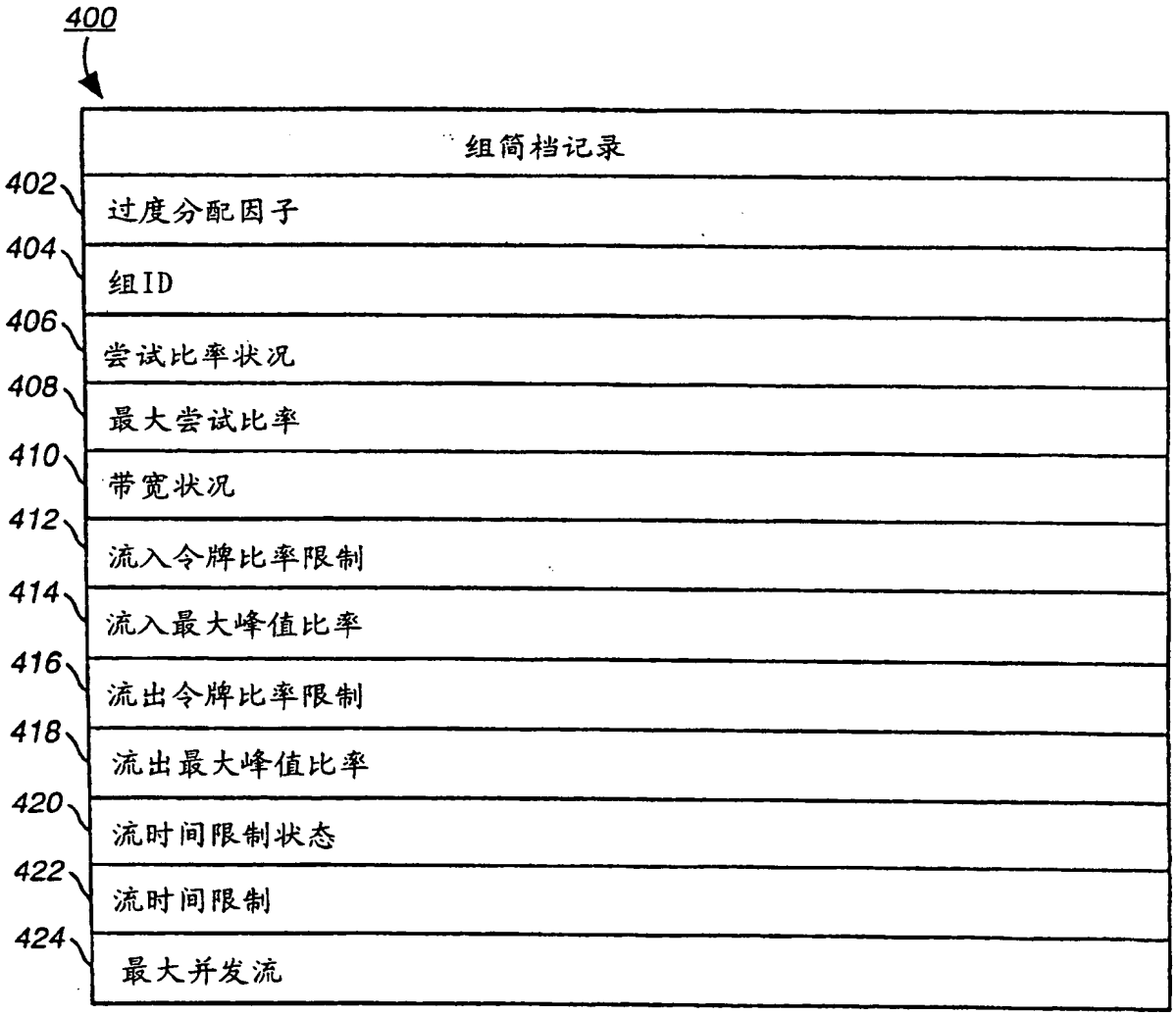

400
组简档记录
402
过度分配因子
404
组ID
406
尝试比率状况
408
最大尝试比率
410
带宽状况
412
流入令牌比率限制
414
流入最大峰值比率
416
流出令牌比率限制
418
流出最大峰值比率
420
流时间限制状态
422
流时间限制
424
最大并发流

图 4

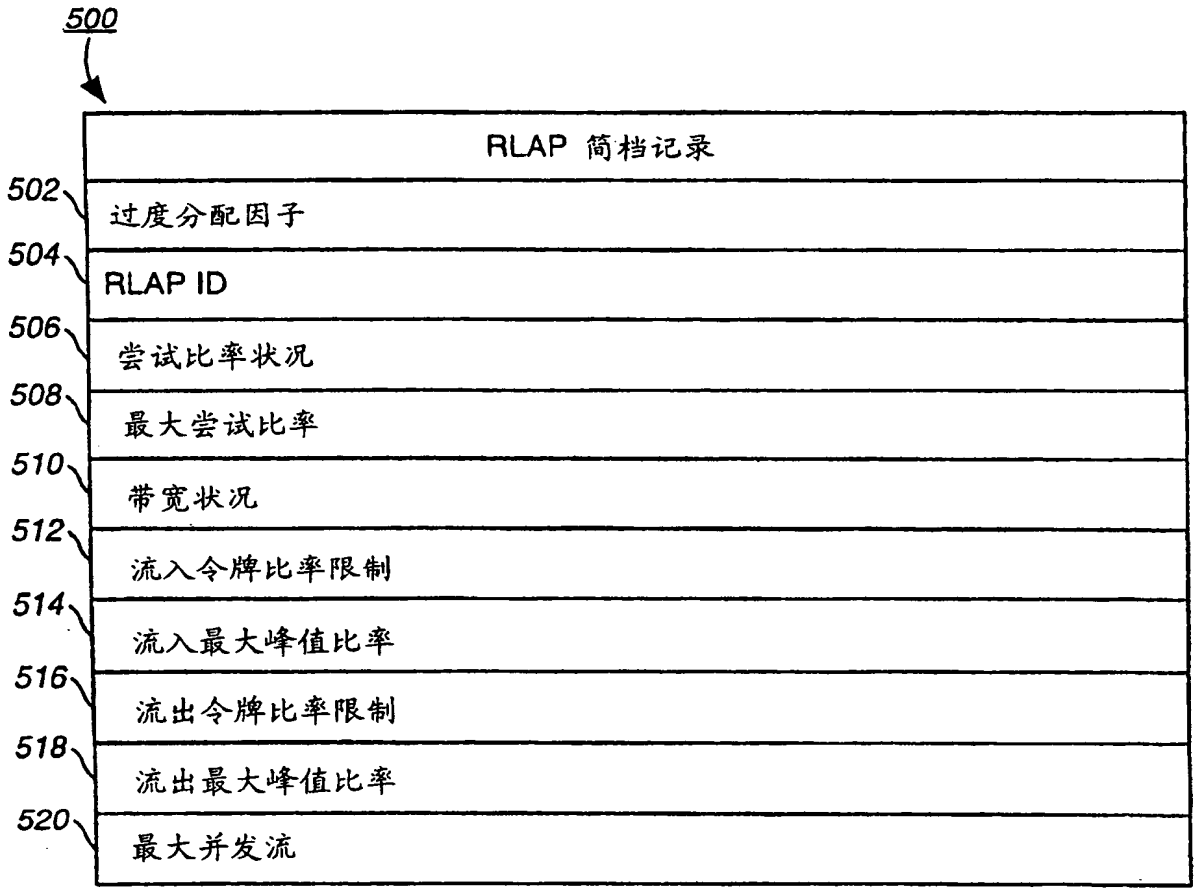

500
RLAP 简档记录
502
过度分配因子
504
RLAP ID
506
尝试比率状况
508
最大尝试比率
510
带宽状况
512
流入令牌比率限制
514
流入最大峰值比率
516
流出令牌比率限制
518
流出最大峰值比率
520
最大并发流

图 5

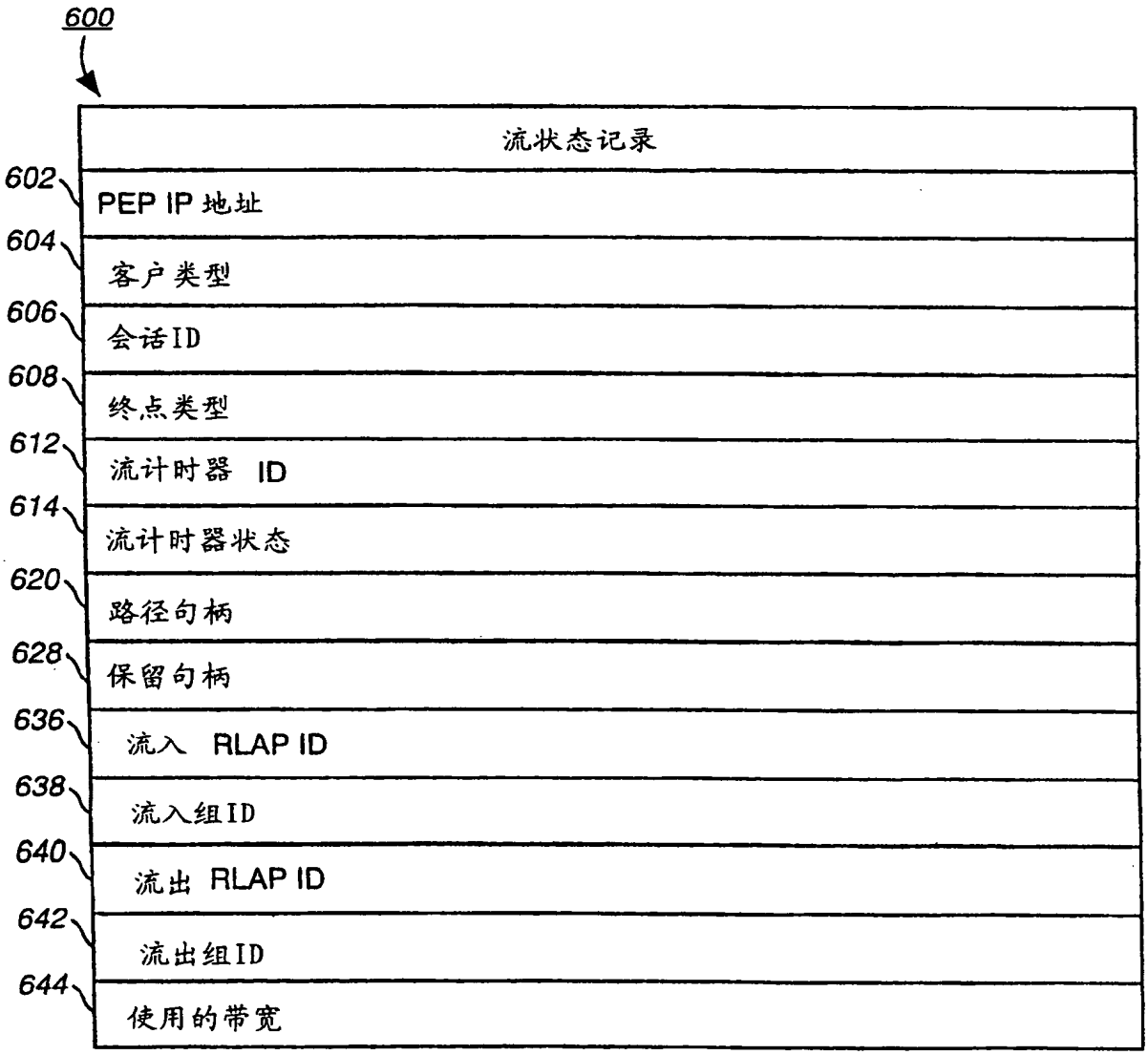

600
流状态记录
602
PEP IP 地址
604
客户类型
606
会话ID
608
终点类型
612
流计时器 ID
614
流计时器状态
620
路径句柄
628
保留句柄
636
流入 RLAP ID
638
流入组ID
640
流出 RLAP ID
642
流出组ID
644
使用的带宽

图 6

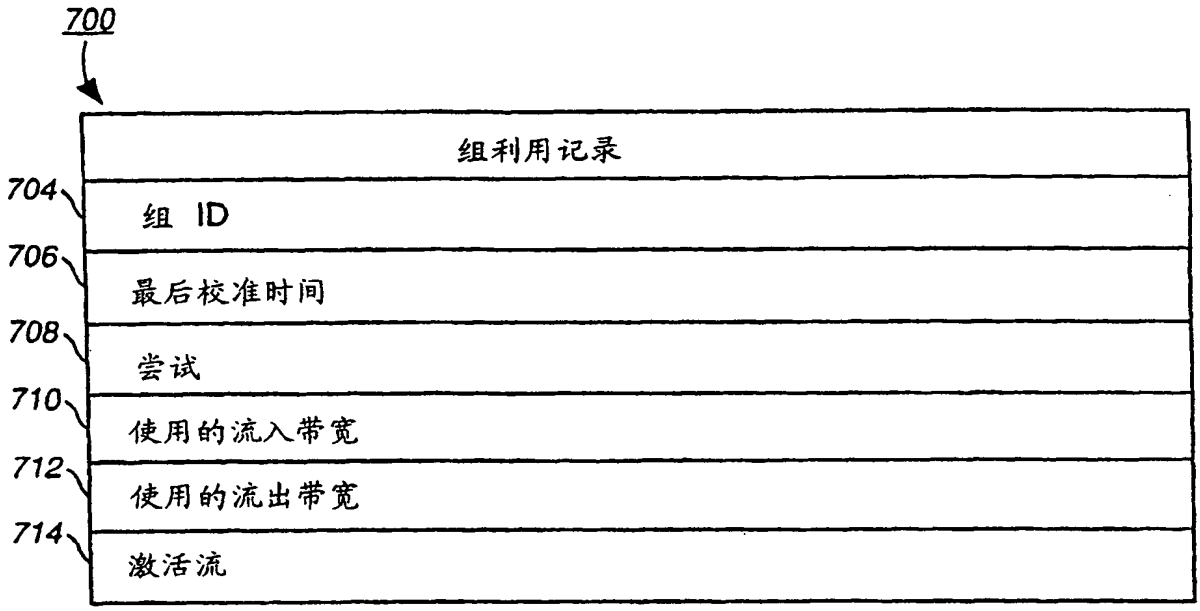

700
组利用记录
704
组 ID
706
最后校准时间
708
尝试
710
使用的流入带宽
712
使用的流出带宽
714
激活流

图 7

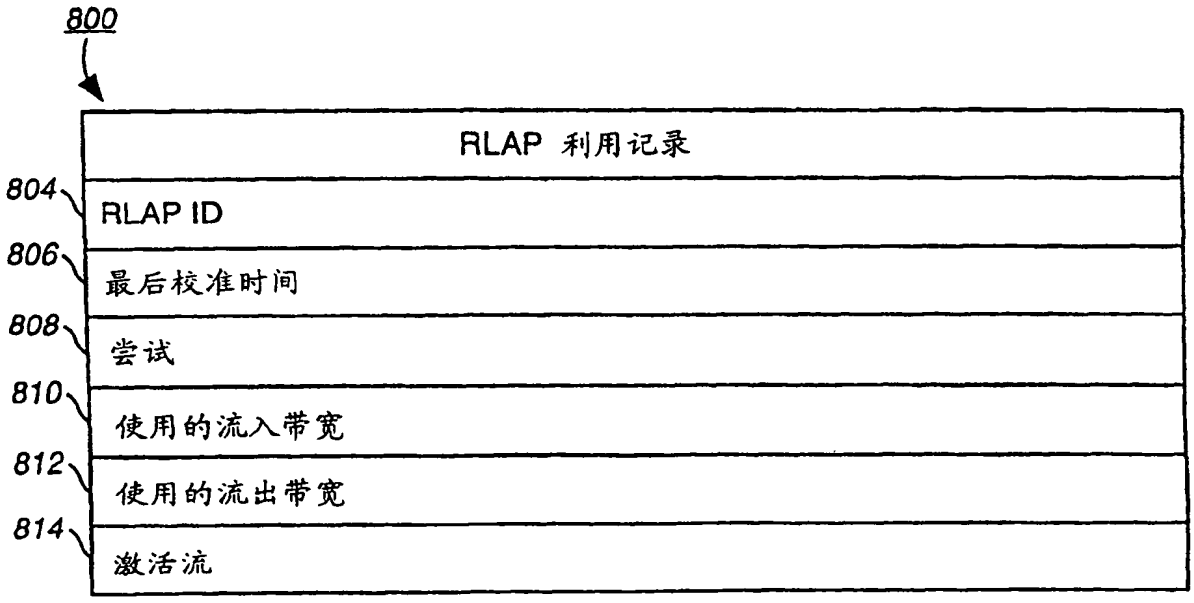

800
RLAP 利用记录
804
RLAP ID
806
最后校准时间
808
尝试
810
使用的流入带宽
812
使用的流出带宽
814
激活流

图 8

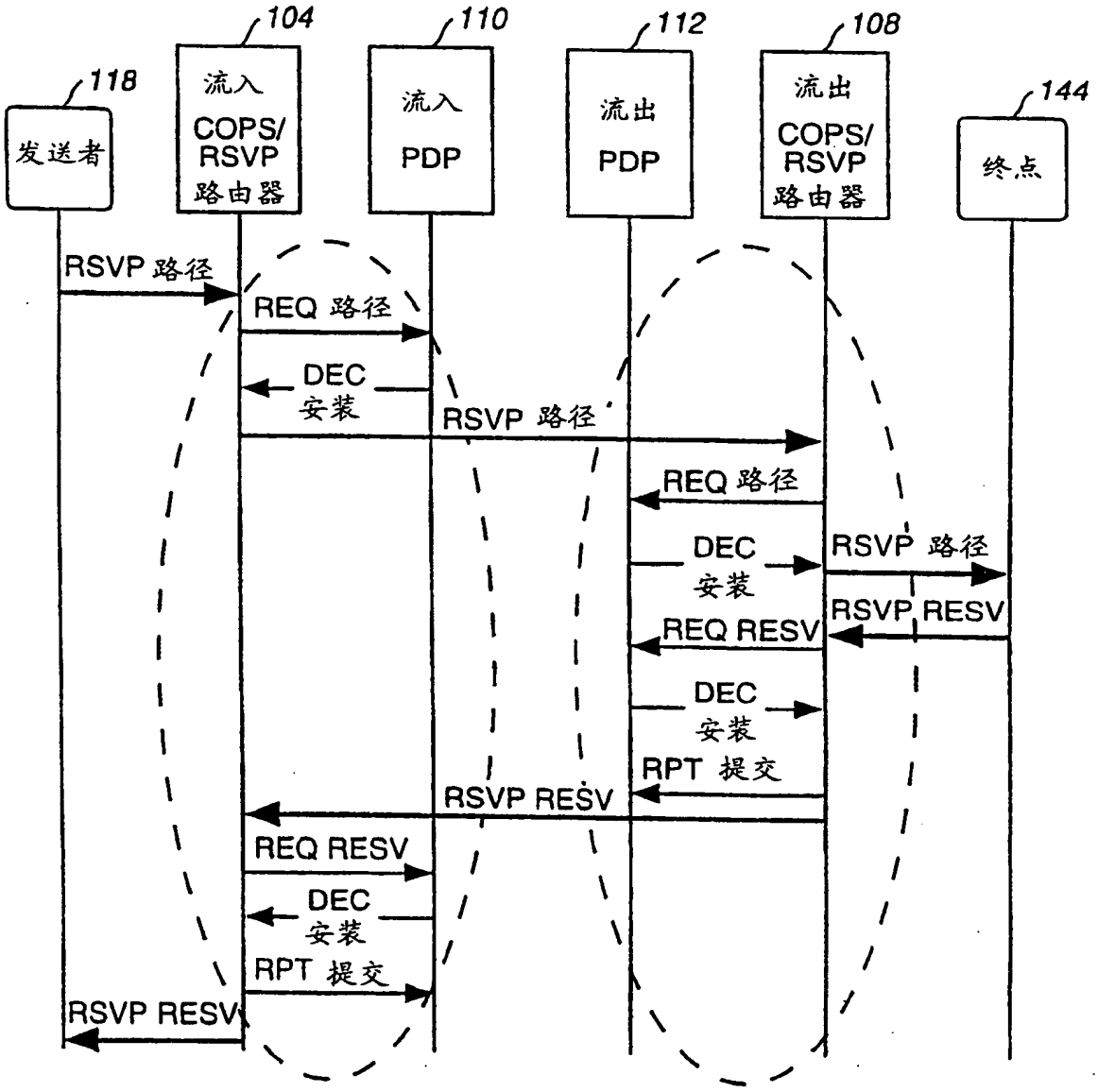

104
110
112
108
118
144
流入
COPS/
RSVP
路由器
流入
PDP
流出
PDP
流出
COPS/
RSVP
路由器
发送者
终点
RSVP 路径
REQ 路径
DEC
安装
RSVP 路径
REQ 路径
DEC
安装
RSVP 路径
RSVP RESV
REQ RESV
DEC
安装
RPT 提交
RSVP RESV
REQ RESV
DEC
安装
RPT 提交
RSVP RESV

图 9

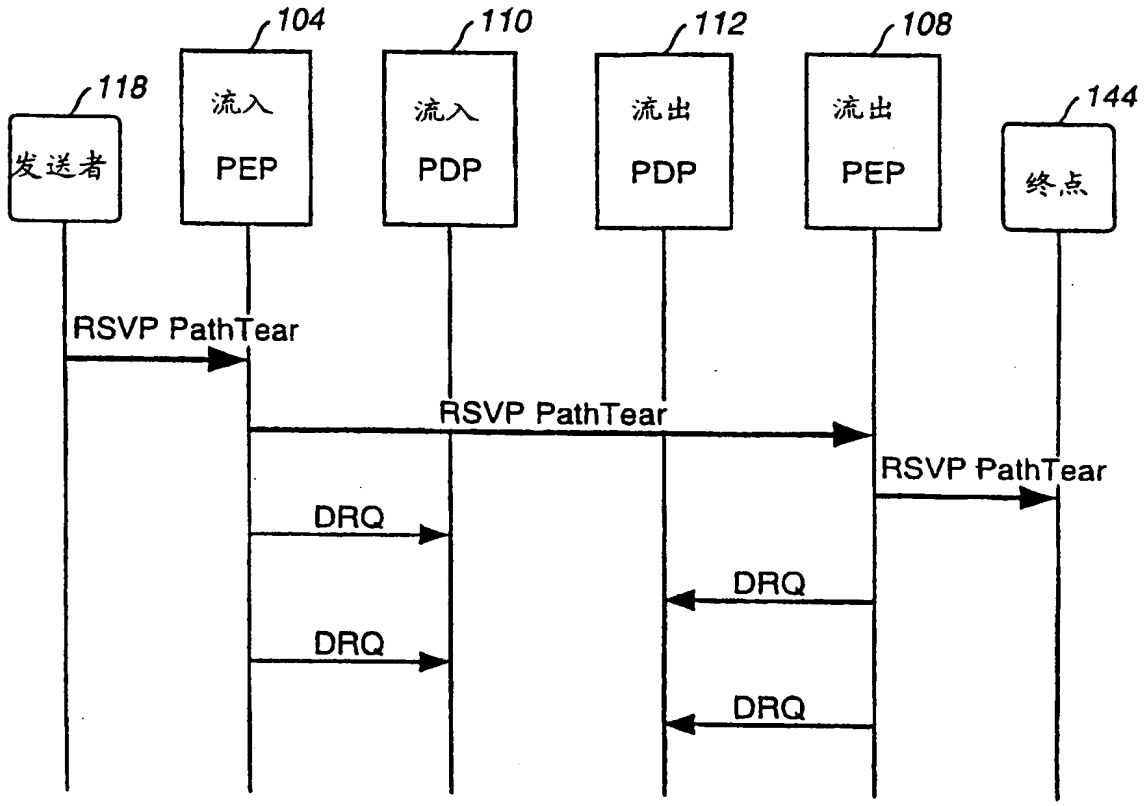

104
110
112
108
118
144
流入
PEP
流入
PDP
流出
PDP
流出
PEP
发送者
终点
RSVP PathTear
RSVP PathTear
RSVP PathTear
DRQ
DRQ
DRQ
DRQ

图 10

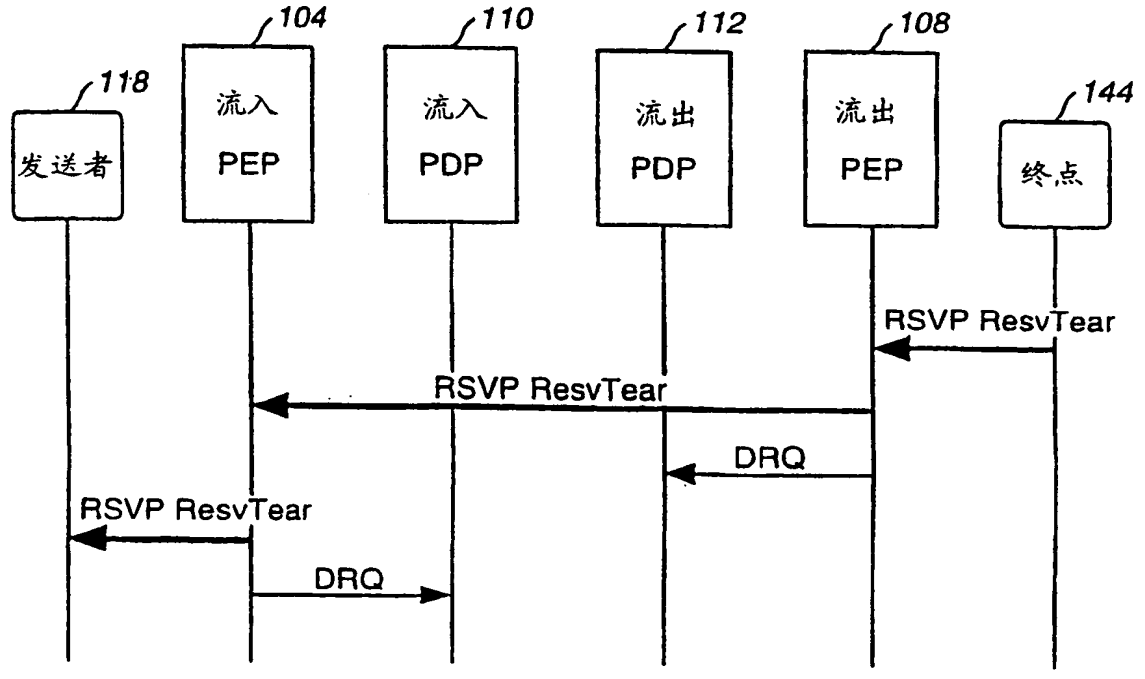

104
110
112
108
118
144
流入
PEP
流入
PDP
流出
PDP
流出
PEP
发送者
终点
RSVP ResvTear
RSVP ResvTear
DRQ
RSVP ResvTear
DRQ

图 11

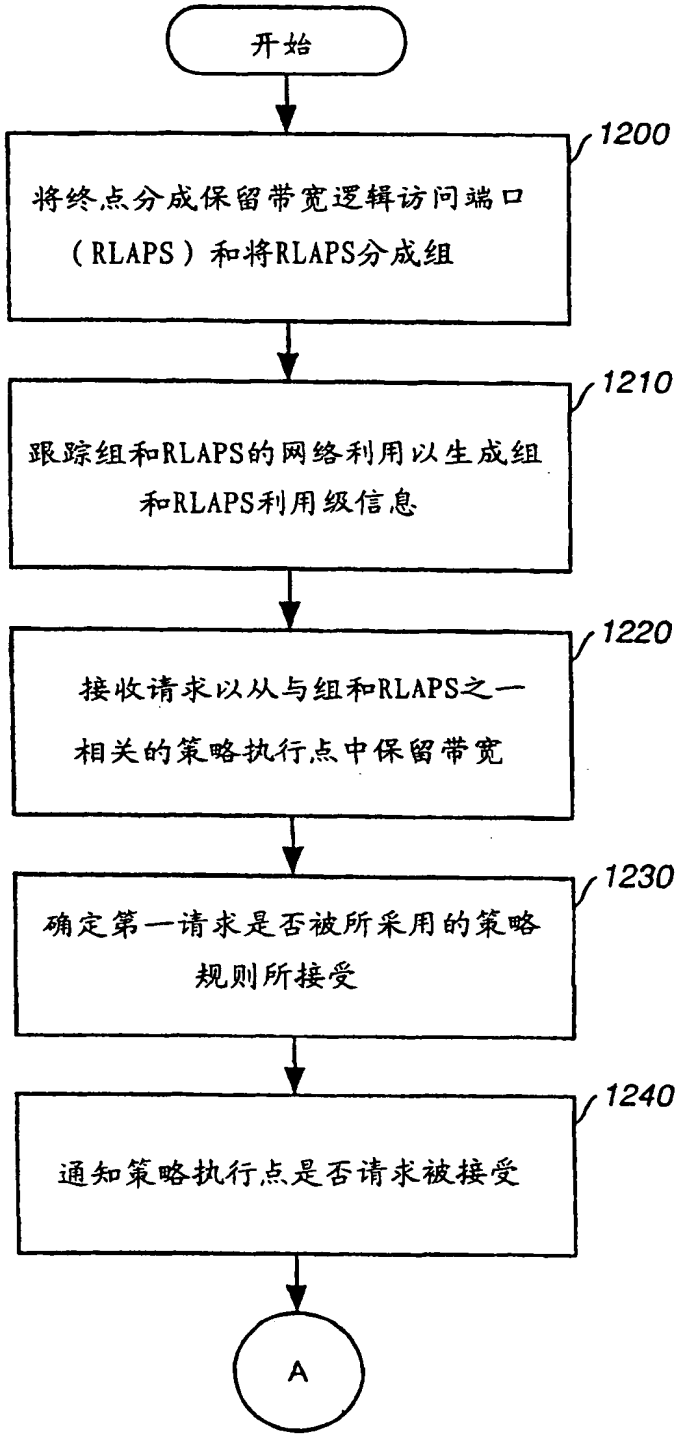

开始
1200
将终点分成保留带宽逻辑访问端口（RLAPS）和将RLAPS分成组
1210
跟踪组和RLAPS的网络利用以生成组和RLAPS利用级信息
1220
接收请求以从与组和RLAPS之一相关的策略执行点中保留带宽
1230
确定第一请求是否被所采用的策略规则所接受
1240
通知策略执行点是否请求被接受
A

图 12

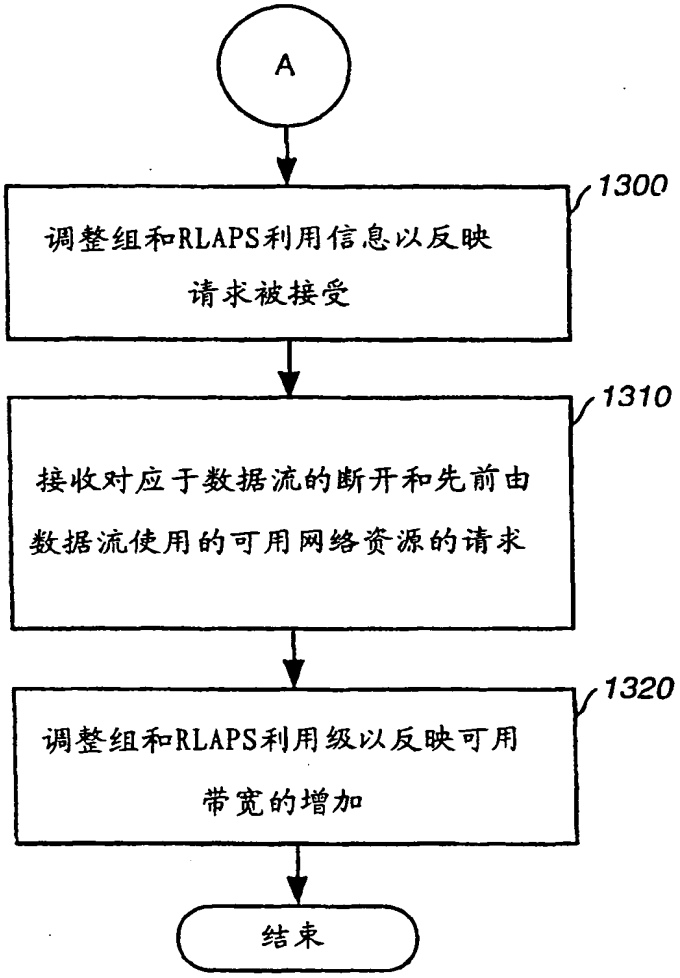

A
1300
调整组和RLAPS利用信息以反映请求被接受
1310
接收对应于数据流的断开和先前由数据流使用的可用网络资源的请求
1320
调整组和RLAPS利用级以反映可用带宽的增加
结束

图 13

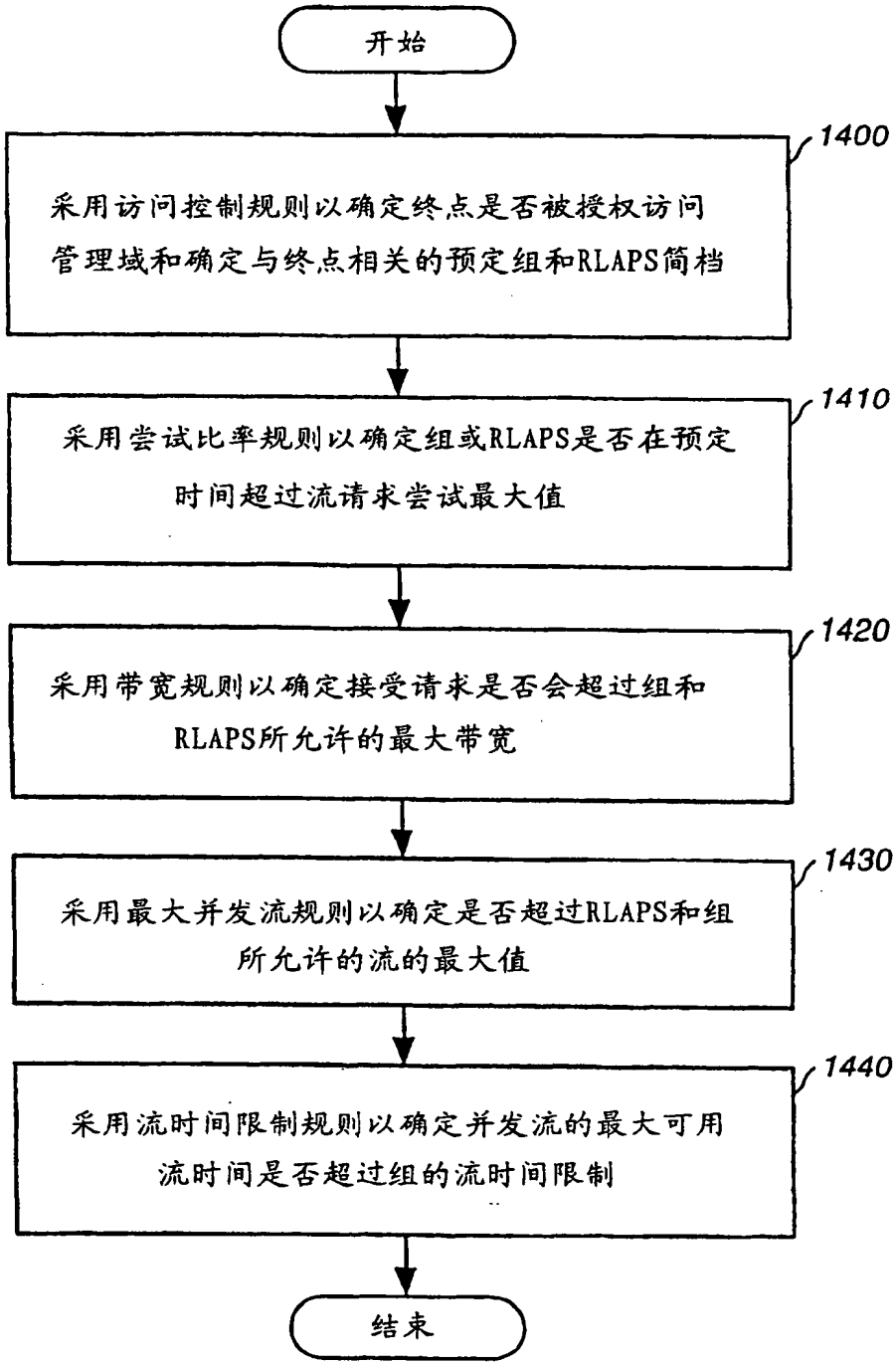

开始
1400
采用访问控制规则以确定终点是否被授权访问管理域和确定与终点相关的预定组和RLAPS简档
1410
采用尝试比率规则以确定组或RLAPS是否在预定时间超过流请求尝试最大值
1420
采用带宽规则以确定接受请求是否会超过组和RLAPS所允许的最大带宽
1430
采用最大并发流规则以确定是否超过RLAPS和组所允许的流的最大值
1440
采用流时间限制规则以确定并发流的最大可用流时间是否超过组的流时间限制
结束

图 14

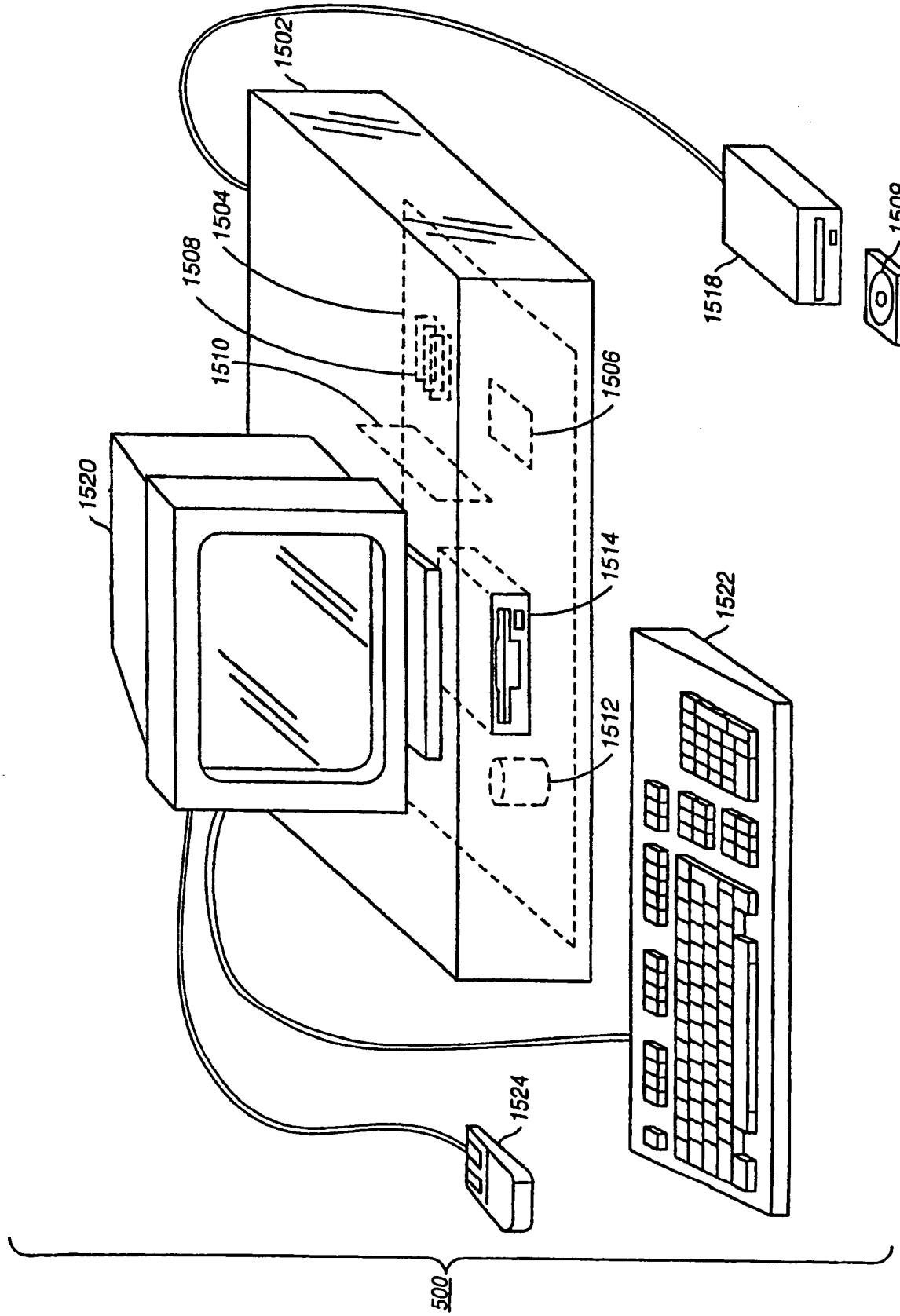

1502
1504
1508
1510
1506
1520
1514
1522
1512
1524
1518
1509
500

图 15